HowTo

Best Practice – Avira Premium Security Suite

Avira Support

Juli 2009

Inhaltsverzeichnis

1. GRUNDWISSEN ZUR FIREWALL 3

2. BEGRIFFSERKLÄRUNG 3

3. EINSTELLUNGSMÖGLICHKEITEN 5

3.1 SICHERHEITSNIVEAU 5
3.1.1 Alle blockieren 7
3.1.2 Benutzer 8
3.1.3 Hoch 8
3.1.4 Mittel 9
3.1.5 Niedrig 10
3.2 KONFIGURATION 10
3.2.1 Adapterregel 11
3.2.1.1 Eingehende Regeln 11
3.2.1.2 Ausgehende Regeln 12
3.2.2 Anwendungsregeln 14
3.2.2.1 Anwendung hinzufügen 14
3.2.2.2 Anwendungseinstellungen 15
3.2.3 Vertrauenswürdige Anbieter 16
3.2.3.1 Vertrauenswürdige Anbieter für Benutzer 17
3.2.3.2 Von vertrauenswürdigen Anbietern erstellte Anwendungen automatisch zulassen 18
3.2.3.3 Anbieter 19
3.2.3.4 Entfernen 20
3.2.3.5 Neu laden 21
3.2.4 Einstellungen 22
3.2.4.1 Zeitüberschreitung der Regel 22
3.2.4.2 Erweiterte Einstellungen 22
3.2.4.3 Benachrichtigungen 23
3.2.4.4 Anwendungsregeln 25
3.2.5 Popup Einstellungen 26
3.2.5.1 Popup Einstellungen 26
3.2.5.2 Aktion für diese Anwendung speichern 27
3.2.5.3 Details anzeigen 28
3.2.5.4 Privilegierte zulassen 29

4. ALLGEMEINES ZUM KINDERSCHUTZ 31

4.1 KINDERSCHUTZ AKTIVIEREN 32
4.2 BENUTZERAUSWAHL 32
4.3 ROLLEN 33
4.3.1 Eigenschaften von Rollen 34

5. ÄNDERUNG DER UPDATE-INTERVALLE 36

5.1 ÄNDERUNG DES UPDATE-AUFTRAGS 36

1. Grundwissen zur Firewall

Eine Firewall arbeitet mit Netzwerkprotokollen wie z.B. TCP, UDP, IP, etc.

Ein einfaches Beispiel für den Verbindungsaufbau des TCP-Protokolls nennt man auch Handshake-Verfahren. Damit soll Ihnen erklärt werden, wie eine Kommunikation von zwei Rechnern im Internet zustande kommt.

- Computer A schickt ein Paket, in dem steht, dass er eine Verbindung zu Computer B aufbauen möchte
- Darauf antwortet Computer B, dass er dazu bereit ist.
- Computer A bestätigt anschließend Computer B, dass er verstanden hat, dass Computer B bereit ist
- Die Verbindung zwischen Computer A und Computer B ist damit hergestellt, und der eigentliche Datenaustausch kann beginnen

2. Begriffserklärung

TCP:
Das *Transmission Control Protocol (TCP)* (zu dt. *Übertragungssteuerungsprotokoll*) ist eine Vereinbarung (Protokoll) darüber, auf welche Art und Weise Daten zwischen Computern ausgetauscht werden sollen.

UDP:
Das *User Datagram Protocol (UDP)* ist ein minimales, verbindungsloses Netzwerkprotokoll.
Um die Daten, die mit UDP versendet werden, dem richtigen Programm auf dem Zielrechner zukommen zu lassen, werden bei UDP sogenannte Ports verwendet. Dazu wird bei UDP die Portnummer des Dienstes mit gesendet, der die Daten erhalten soll. Zusätzlich bietet UDP die Möglichkeit, einer Integritätsüberprüfung an, indem eine Prüfsumme mit gesendet wird. Dadurch kann eine fehlerhafte Übertragung erkannt werden.

Flooding:
Flooding (engl. überfluten) bezeichnet das Überschwemmen eines Netzwerkes mit Paketen. Flooding kann den Datenverkehr in einem Netzwerk (oder eines einzelnen Rechners) lahm legen, da der Rechner oder das Netzwerk mit einer Masse von Anfragen überschwemmt wird und dadurch nicht mehr reagieren kann. Man kann dies mit einem Stau auf der Autobahn vergleichen.

Ports:
Einen *Port* kann man mit einer Hausnummer vergleichen. Nur ist der Unterschied, dass ein Haus, in diesem Falle der Computer, auch mehrere Nummern haben kann.

Ein Port ist ein Teil einer Adresse, welcher ankommende Pakete einer Anwendung zuordnet.
Beispiel hierfür:
Port 110, zuständig für Dienst POP3, gewährleistet den Zugriff auf den Email-Server. Bestimmte Applikationen verwenden Portnummern, die ihnen von der IANA fest zugeordnet und allgemein bekannt sind. Sie liegen üblicherweise von 0 bis 1023, und werden als *Well Known Ports* bezeichnet. Von Port 1024 bis 49151 befinden sich die *Registered Ports*. Anwendungshersteller können bei Bedarf Ports für eigene Protokolle registrieren lassen, ähnlich wie Domainnamen. Die Registrierung hat den Vorteil, dass eine Anwendung anhand der Portnummer identifiziert werden kann, allerdings nur wenn die Anwendung auch den bei der IANA eingetragenen Port verwendet. Die restlichen Ports von Portnummer 49152 bis 65535 sind so genannte *Dynamic* und/oder *Private Ports*. Weitere Informationen finden Sie unter folgendem Link:
http://www.iana.org/assignments/port-numbers

Portscan:
Portscans werden unter anderem ausgeführt um freie Ports auf dem Rechner auszuspähen.
Wenn ein Rechner, einen Serverdienst für andere zur Verfügung stellt, öffnet er einen TCP/IP- oder UDP-Port, oder auch beides oder mehrere. Ein Webserver muss den Port 80 geöffnet haben. Ein Portscan ermittelt nun, welche Ports auf dem Rechner geöffnet sind. Um zu überprüfen, welche Ports auf Ihrem Rechner gerade geöffnet sind, können Sie einen Test unter folgenden Link durchführen:
http://www.port-scan.de/index2.php

IP:
Um einen bestimmten Computer ansprechen zu können, identifiziert ihn das *Internetprotokoll (IP)* mit einer eindeutigen IP-Adresse. Wenn Sie an einen Freund einen Brief schicken möchten, müssen Sie die Straße und den Ort angeben. Genau so funktioniert es auch mit der IP-Adresse.

Host Datei:
Manchmal wird die Hosts-Datei dazu verwendet, bekannte Werbeserver zu blockieren, indem der Localhost (127.0.0.1) eingetragen wird, damit alle Anfragen an das eigene System gesendet werden. Die Besonderheit dieser Methode gegenüber den zu installierenden Werbefiltern ist, dass diese Sperrung systemweit Gültigkeit hat, also nicht nur auf einen Browser beschränkt ist. Darüber hinaus kann man solche Filter auch gegen manche Schadprogramme einsetzen, wenn diese Anweisungen von bereits bekannten Servern abzurufen versuchen.

URL:
Als **Uniform Resource Locator** (**URL**, dt. „einheitlicher Quellenanzeiger“) bezeichnet man eine Unterart von Uniform Resource Identifiern (URIs). URLs identifizieren und lokalisieren eine Ressource über das verwendete Netzwerkprotokoll (beispielsweise HTTP oder FTP) und den Ort (engl. *location*) der Ressource in Computernetzwerken.

Da URLs die erste und häufigste Art von URIs darstellen, werden die Begriffe häufig synonym verwendet.
In der Umgangssprache wird URL häufig als Synonym für Internetadresse wie z.B. www.avira.de verwendet.

Slide-Up:
Als Slide-Up versteht man ein kleines Fenster, dass entweder rechts oben oder rechts unten, langsam auf ihrem Bildschirm erscheint und nach einer Eingabe (Interaktion) oder nach einer gewissen Zeit selbstständig wieder verschwindet.

3. Einstellungsmöglichkeiten

3.1 Sicherheitsniveau

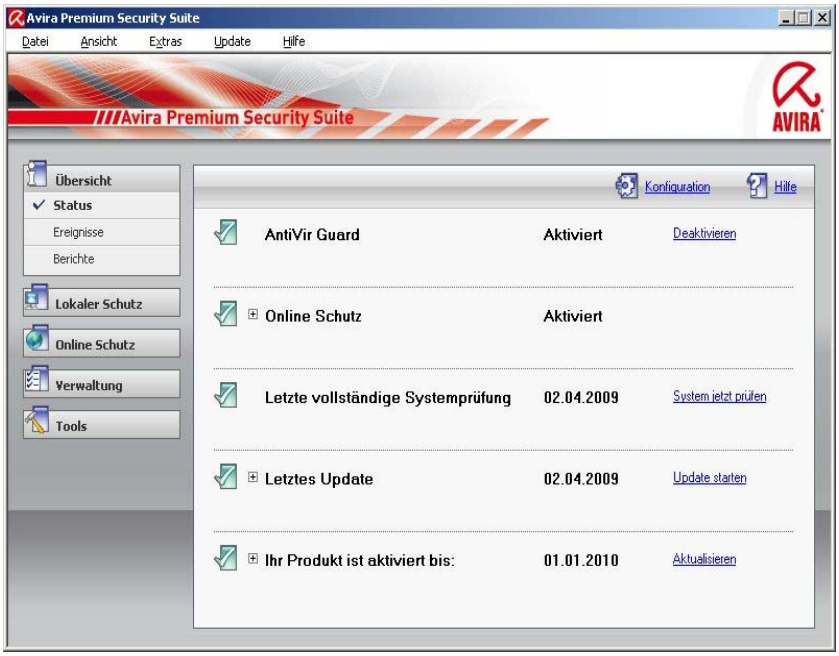
Zuerst gilt es zu entscheiden, welches Sicherheitsniveau eingestellt werden sollte. Eine zu hohe Einstellung des Sicherheitsniveaus kann dazu führen, dass bestimmte Systemfunktionen nicht mehr gewährleistet sind. Eine zu niedrige Einstellung dagegen kann bewirken, dass die Firewall nicht alle Zugriffe auf Ihren Rechner blockiert.

Allgemein gilt: Ist der PC nicht an ein lokales Netzwerk angeschlossen und befindet sich kein netzwerkfähiges Gerät (z.B. Netzwerkdrucker) in der Umgebung des PCs, kann das Sicherheitsniveau auf "Hoch" eingestellt bleiben. Das bedeutet, der Computer ist im Netzwerk unsichtbar. Des Weiteren werden Verbindungen von außen blockiert und Flooding und Portscan verhindert. Dies ist die Standardeinstellung nach der Installation der Avira Premium Security Suite.

Sollte sich der PC jedoch in einer Netzwerkumgebung befinden oder der PC auf Netzwerkgeräte wie z.B. Netzwerkdrucker zugreifen, sollte das Sicherheitsniveau auf "Mittel" gestellt werden. Weil es unter Umständen dazu führen kann, dass der Netzwerkdrucker blockiert wird bzw. nicht erkannt wird, da Sie der Firewall nicht mitgeteilt haben, dass ein Drucker vorhanden ist.

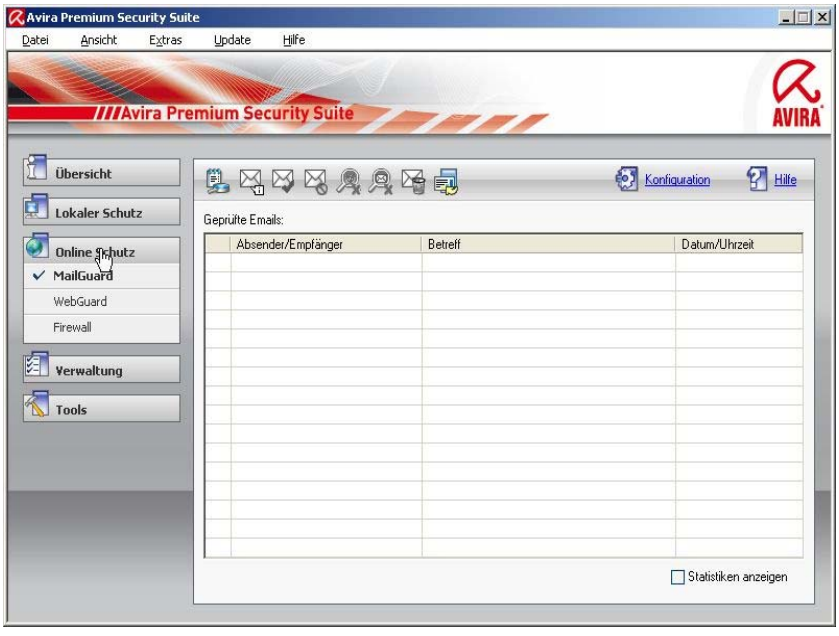
Hierzu gehen Sie wie folgt vor:

- Avira AntiVir Control Center starten



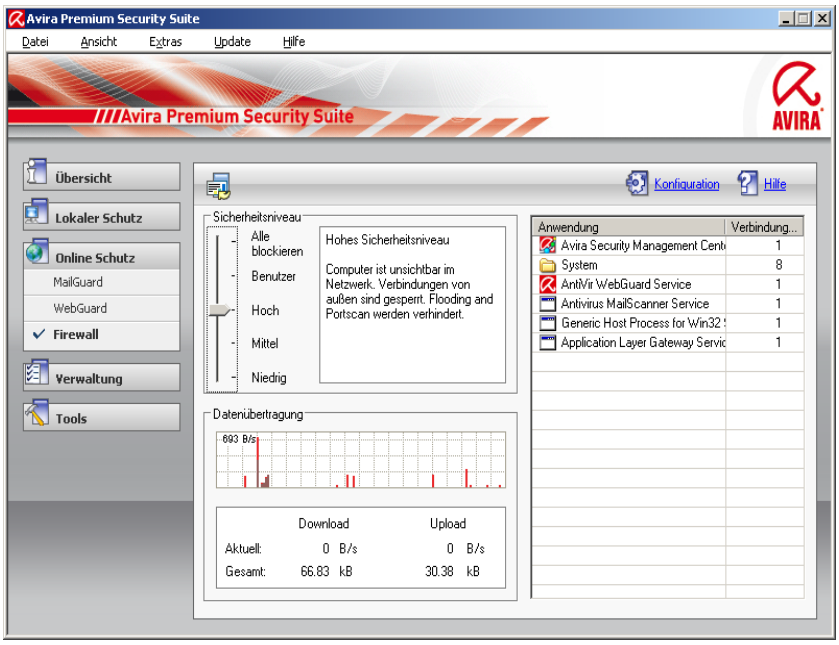
Dies wird am einfachsten durch einen Doppelklick mit der linken Maustaste auf das Schirmsymbol erreicht. Das Trayicon befindet sich in der Taskleiste, unten rechts neben der Systemuhrzeit. Alternativ kann das Control Center über einen Doppelklick auf das bei der Installation angelegten Icons auf dem Desktop gestartet werden.

- Register "Online Schutz" öffnen



Durch einen Klick mit der linken Maustaste auf das Register "Online Schutz" wird dieses aufgeklappt. Das Register "Online Schutz" befindet sich vertikal auf der linken Seite des Control Centers.

- Firewall-Einstellungen öffnen



Ein Klick auf "Firewall" im Untermenü "Online Schutz" öffnet die Konfiguration der Avira Firewall. Diese erscheint rechts im Hauptfenster des Control Centers.

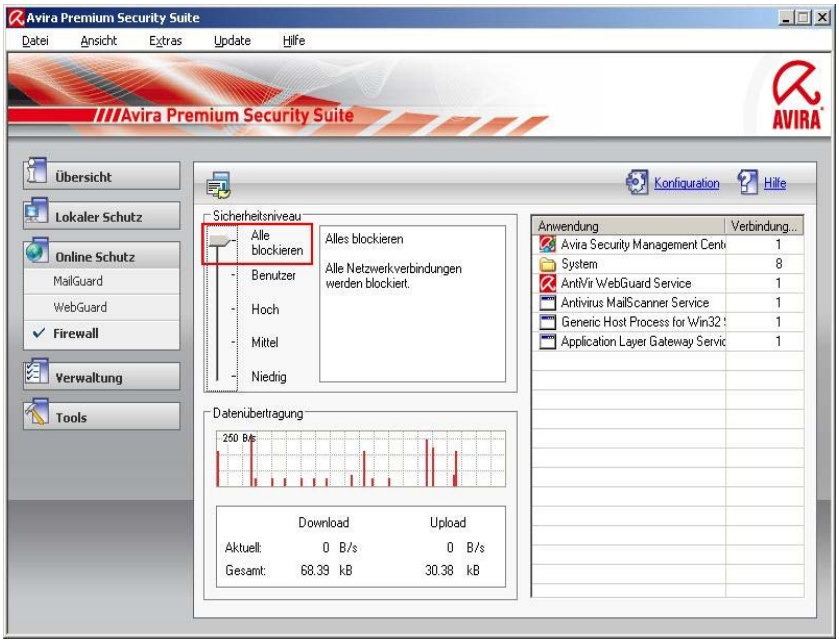
- Sicherheitsniveau der Firewall anpassen

Durch Anklicken und Festhalten des Sicherheitsniveau-Reglers der Firewall lässt sich diese anpassen. Die möglichen Stufen sind "Niedrig", "Mittel", "Hoch", "Benutzer" und "Alle blockieren". Eine Beschreibung der Stufen finden Sie direkt rechts neben dem Sicherheitsniveau-Schieber.

Stellen Sie hier das Niveau auf "Mittel", falls Probleme mit Netzwerkdruckern, externen Festplatten oder ähnlichen Netzwerkverbindungen auftreten sollten.

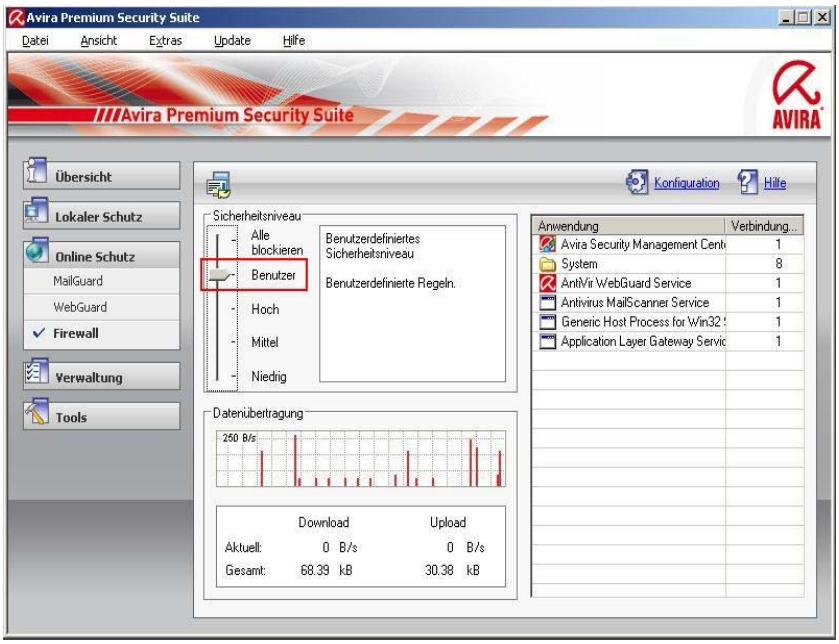
3.1.1 Alle blockieren

Alle Netzwerkverbindungen werden blockiert.



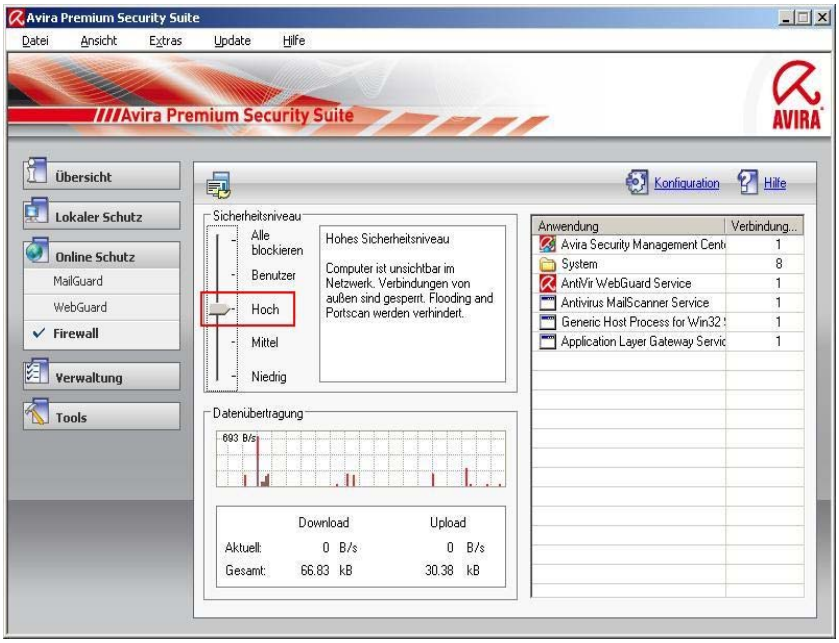
3.1.2 Benutzer

Benutzerdefinierte Regeln können Sie in der Konfiguration einstellen (siehe Seite 10, Kapitel 3.2 Konfiguration).



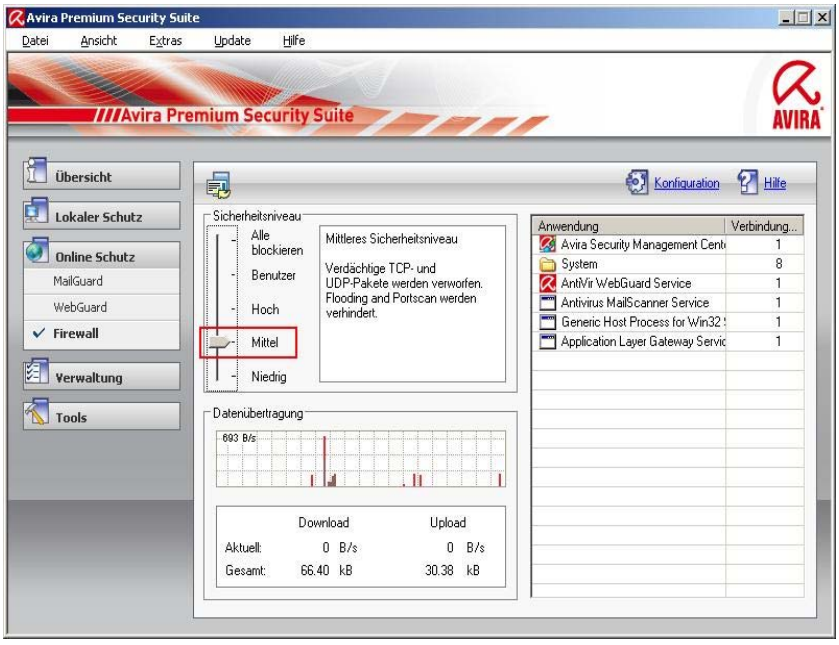
3.1.3 Hoch

Der Computer ist im Netzwerk unsichtbar und die Verbindungen von außen werden blockiert. Flooding und Portscan werden verhindert.



3.1.4 Mittel

Im Vergleich zur Firewalleinstellung „Hoch“, ist der Rechner im Netzwerk sichtbar und bekommt somit TCP- und UDP Anfragen. Diese werden aber verworfen. TCP- und UDP-Pakete, die unerwartet eintreffen oder empfangen werden, werden nicht bearbeitet und nicht entgegengenommen. Flooding und Portscan werden verhindert.

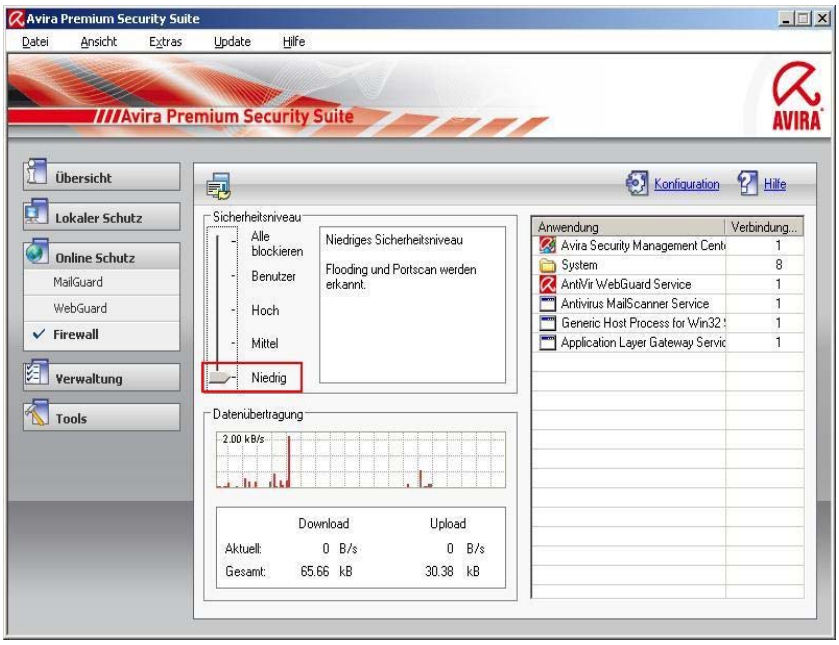


Auch unter der Stufe „Mittel“ können gegebenenfalls Probleme mit dem Netzwerk auftreten. In diesem Fall sollten Sie das Level auf „Niedrig“ heruntersetzen.

Das Preset Level (vorkonfigurierte Regeln) ist unter dem Sicherheitsniveau „Mittel“ ein wenig ausgeprägter, d.h. unter „Mittel“ werden verschiedene TCP und UDP-Paketanfragen erkannt und automatisch verarbeitet. Andere werden verworfen.

3.1.5 Niedrig

Auch unter der Stufe „Niedrig“ haben Sie noch den Schutz der Avira Firewall. Es werden nicht wie bei der Stufe „Mittel“ Flooding und Portscan verhindert, sondern nur noch erkannt. Dies sind die gängigsten Arten, eine „Lücke“ auf Ihrem Rechner ausfindig zu machen.

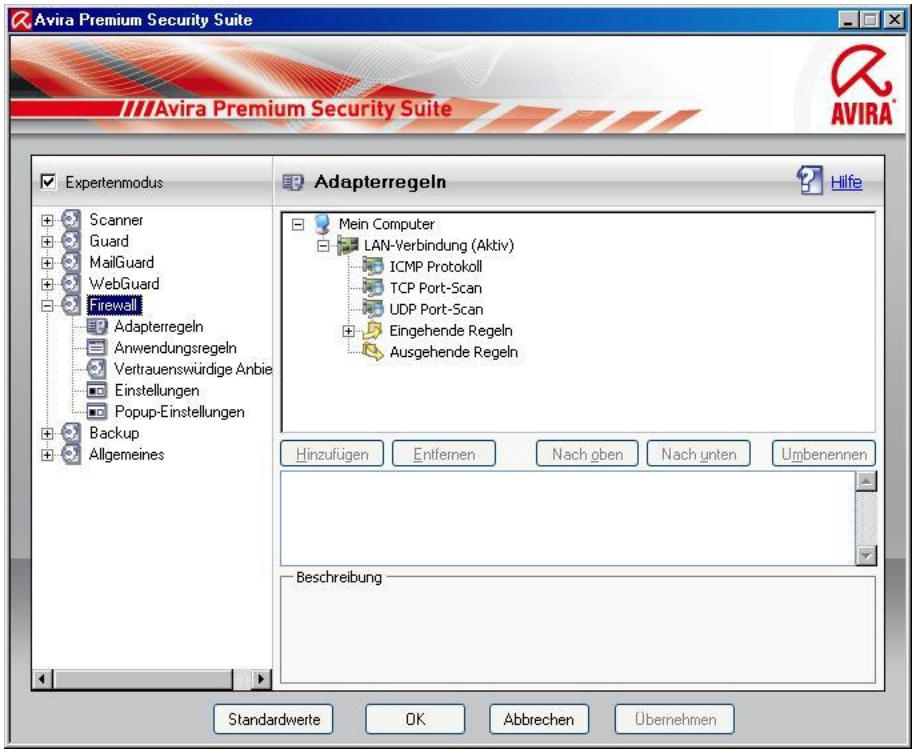


Sind die Einstellungen für Sie nicht ausreichend oder verschiedene Ports müssen für eine Anwendung frei geschaltet werden, so können Sie unter Punkt *3.2 Konfiguration* weitere Einstellungen vornehmen.

3.2 Konfiguration

Klicken Sie mit der rechten Maustaste auf das Trayicon in der Taskleiste und wählen Sie den Punkt „AntiVir konfigurieren“ aus. Sie haben auch die Möglichkeit, über das Avira AntiVir Control Center die Konfiguration zu starten, indem sie das Control Center öffnen und oben rechts auf „Konfiguration“ klicken, oder F8 drücken, oder über Extras –> Konfiguration gehen.

In der Konfiguration finden Sie auf der linken Seite den Punkt „Firewall“. Aktivieren Sie den Expertenmodus, um alle Einstellungen sehen und ändern zu können. Hier können Sie die *Adapterregeln*, *Anwendungsregeln*, *Vertrauenswürdige Anbieter*, allgemeine *Einstellungen* und *Popup Einstellungen* konfigurieren.



3.2.1 Adapterregel

Als Adapter wird in der Avira Firewall jede von einer Software **simulierte** Hardwareeinheit (z.B. Miniport, Bridge Connection, usw.) oder jede Hardwareeinheit (z.B. eine Netzwerkkarte) betrachtet.
Die Avira Firewall zeigt die Adapterregeln für alle auf Ihrem Computer existierenden Adapter an, für die ein Treiber installiert ist.

Eine vordefinierte Adapterregel ist abhängig vom Sicherheitsniveau. Sie können das Sicherheitsniveau über das Avira Control Center wie unter Punkt 3.1 beschrieben ändern, oder die Adapterregeln auf Ihre Bedürfnisse anpassen. Haben Sie die Adapterregeln auf Ihre Bedürfnisse angepasst, wird unter der Rubrik Firewall des Avira Premium Security Suite Control Center im Bereich Sicherheitsniveau der Regler auf Benutzer platziert.

3.2.1.1 Eingehende Regeln

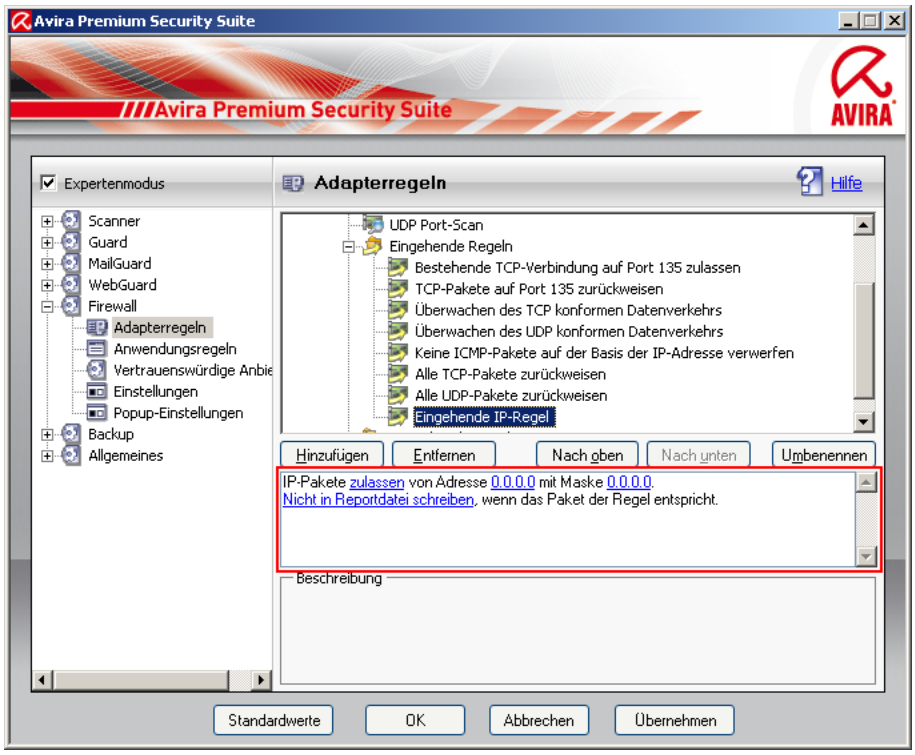
Eingehende Regeln dienen zur Kontrolle des eingehenden Datenverkehrs durch die Avira Firewall.

Beispiel:

Sie wollen die IP- Adresse 10.40.30.20 hinzufügen.

Wenn Sie auf „Hinzufügen“ klicken, öffnet sich ein neues Fenster mit verschiedenen vordefinierten Regeln. Dort wählen Sie „IP“ aus und bestätigen mit „OK“.

In Ihren „Eingehenden Regeln“ finden Sie nun den Punkt „eingehende IP-Regel“. Wählen Sie diesen aus. Sie können den Punkt auch umbenennen.
Sie können nun im unten markierten Kasten die IP und deren Maske eintragen und diese entweder zulassen oder sperren. Ebenso können Sie entscheiden, ob das Paket in die Reportdatei geschrieben werden soll oder nicht.



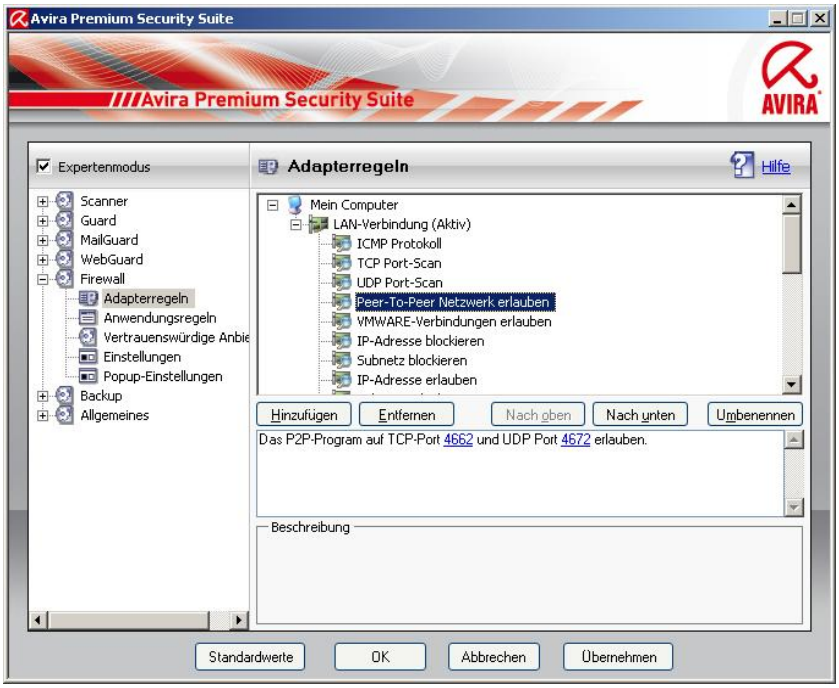
3.2.1.2 Ausgehende Regeln

Ausgehende Regeln dienen zur Kontrolle des ausgehenden Datenverkehrs durch die Avira Firewall. Sie können eine ausgehende Regel für die folgenden Protokolle definieren: IP, ICMP, UDP und TCP. Um Einstellungen zur „Ausgehenden Regel“ vorzunehmen, gehen Sie genauso vor wie bei der „Eingehenden Regel“.

Beispiele:

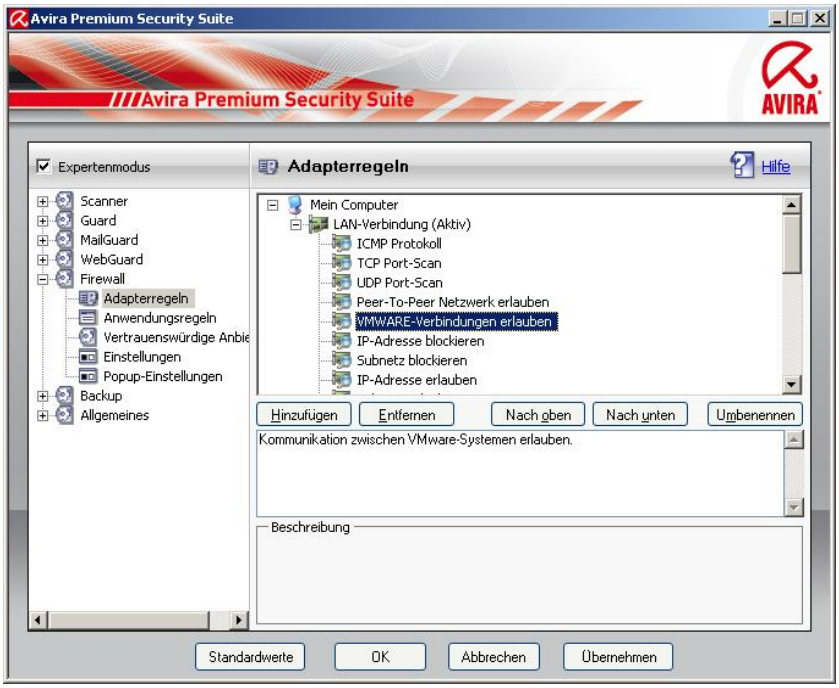
- Peer to Peer

Sollten Sie z.B. Tauschsysteme, Dateisysteme oder File-Sharing-Systeme verwenden, können Sie dieses vorgefertigte Template verwenden. Sie müssen in diesem Fall nur noch die benötigten TCP- und UDP-Ports freigeben.



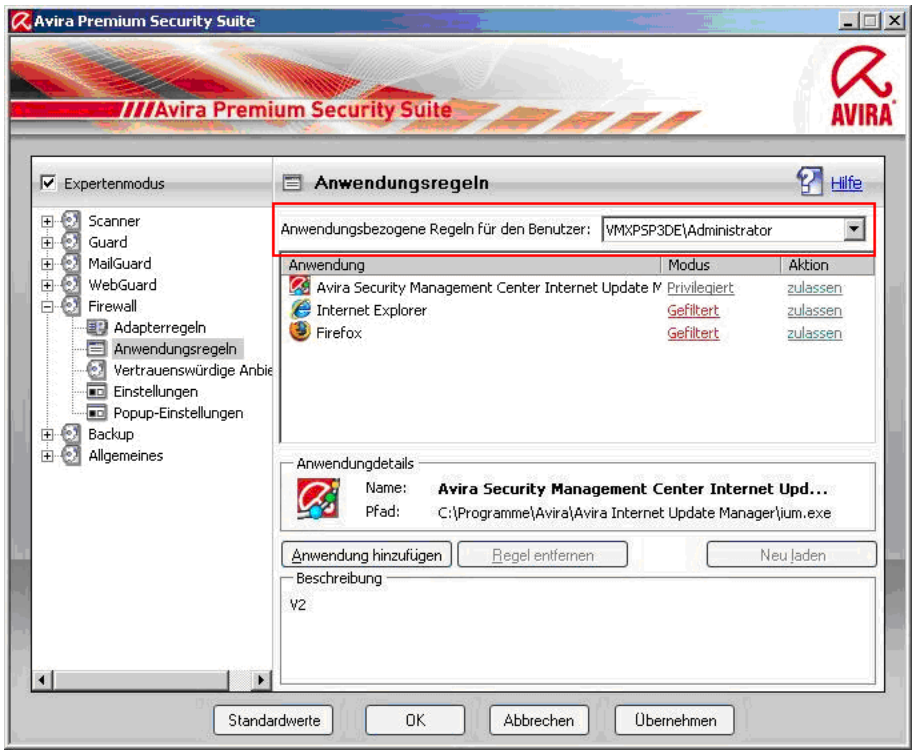
- VMware

Sollte der Internetzugriff von Ihrer VMware nicht möglich sein, müssen Sie diese über folgendes Template freischalten.



3.2.2 Anwendungsregeln

Diese Liste enthält alle Anwender im System. Falls Sie als Administrator angemeldet sind, können Sie einen Benutzer auswählen, für den Sie Regeln erstellen möchten. Falls Sie kein Anwender mit privilegierten Rechten sind, zeigt Ihnen die Liste nur den aktuell angemeldeten Benutzer.



Beispiel:
So kann ein Administrator dafür sorgen, dass ein Webbrowser keinen Internetzugriff erhält, oder ein Chatprogramm nicht ausgeführt werden kann.

3.2.2.1 Anwendung hinzufügen

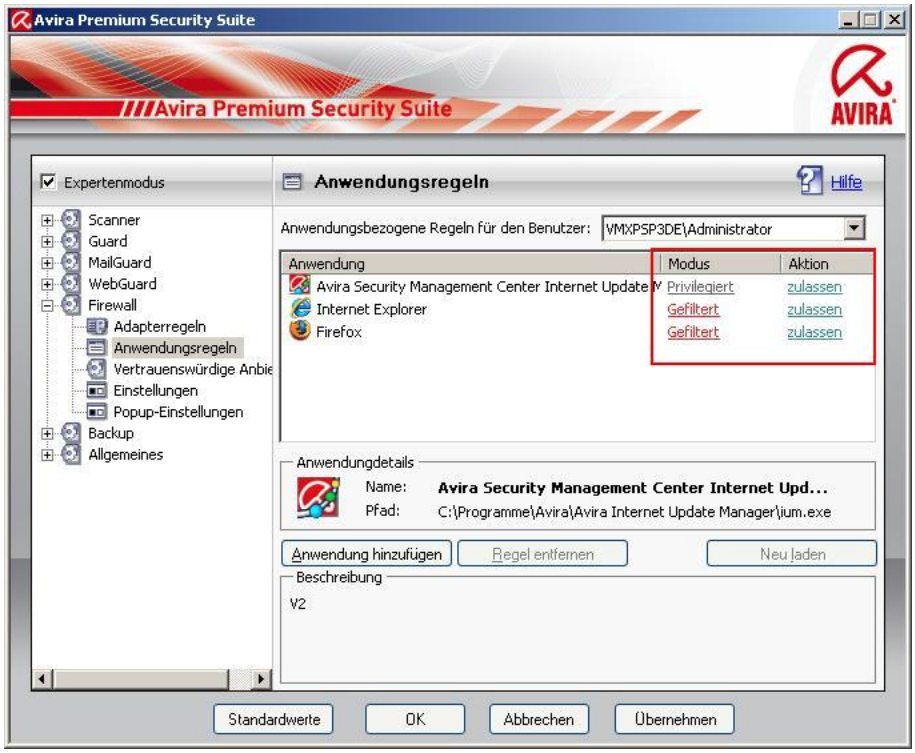
Wenn Sie auf den Button „Anwendung hinzufügen“ klicken, öffnet sich ein neues Fenster mit den Programmen, die auf Ihrem Rechner installiert sind.

Durch einfaches Anklicken wird die Anwendung markiert und kann von Ihnen über den Button „Hinzufügen“ zur Liste aufgenommen werden.

3.2.2.2 Anwendungseinstellungen

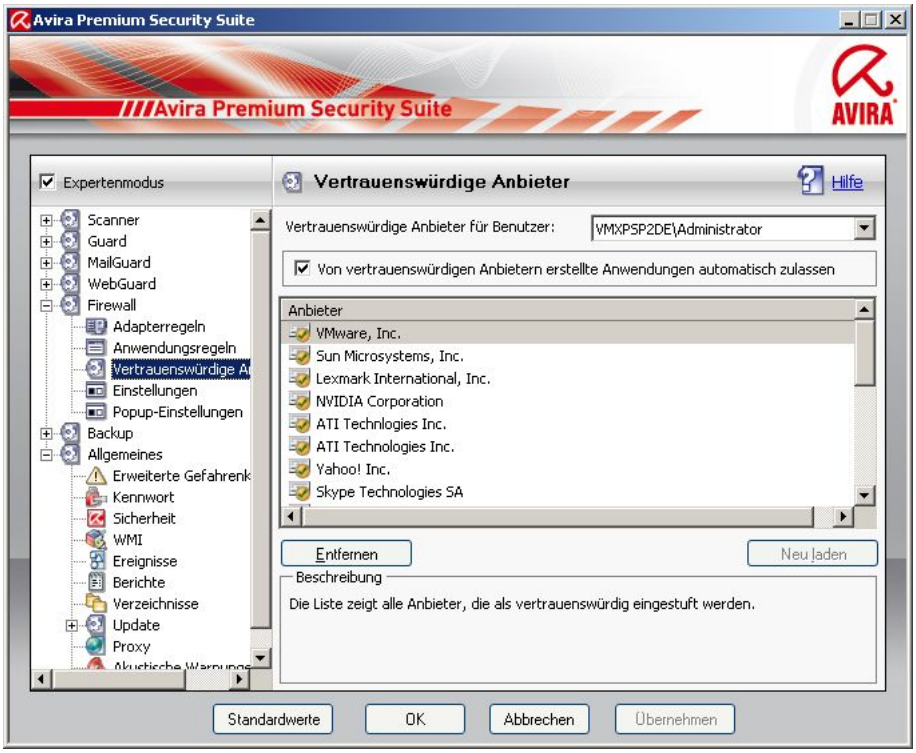
Dort können Sie den Modus von „Gefiltert“ zu „Privilegiert“ ändern. Bei gefiltertem Modus werden die Adapterregeln und die Anwendungsregeln überprüft, hingegen zum privilegierten Modus werden nur die Anwendungsregeln kontrolliert.

Ebenso kann die Aktion von „zulassen“ auf „zurückweisen“ oder „fragen“ geändert werden. Stellen Sie die Aktion auf „fragen“, werden Sie immer vor der Ausführung des Programms von AntiVir gefragt, ob Sie wirklich das Programm starten wollen. Bei „zurückweisen“ wird das Programm von der Avira Firewall geblockt.



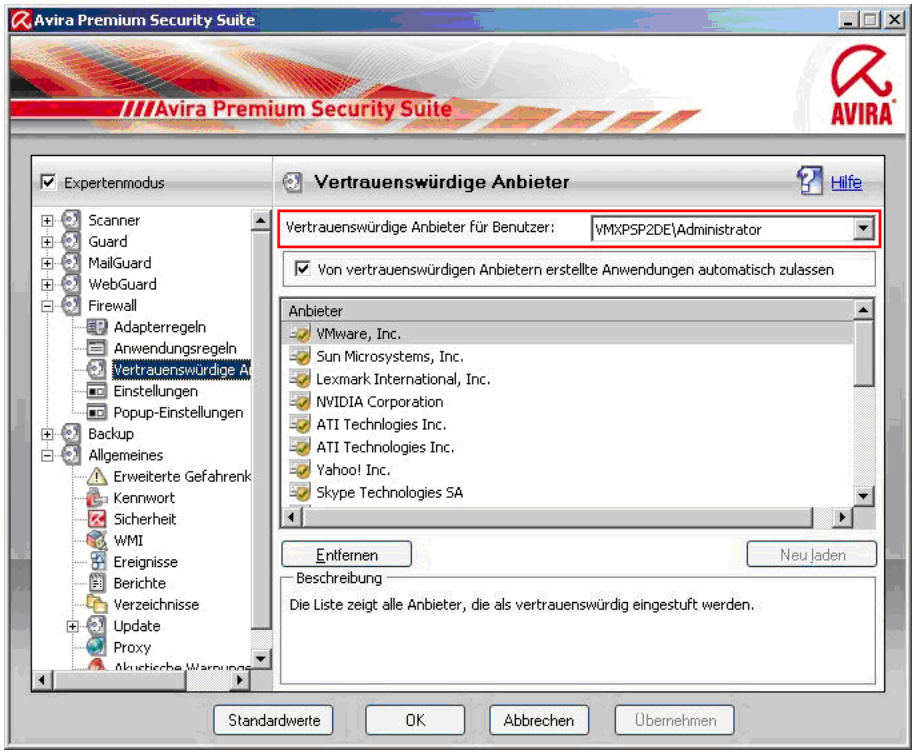
3.2.3 Vertrauenswürdige Anbieter

Unter „Vertrauenswürdige Anbieter“ wird eine Liste von vertrauenswürdigen Software-Herstellern angezeigt. Sie können Hersteller aus der Liste entfernen oder hinzufügen, indem Sie die Option „Diesem Anbieter immer vertrauen“ im Popup-Fenster Netzwerkereignis nutzen. Sie können den Netzzugriff von Anwendungen, die von den aufgelisteten Anbietern signiert sind, standardmäßig erlauben, indem Sie die Option „Von vertrauenswürdigen Anbietern erstellte Anwendungen automatisch zulassen“ aktivieren.



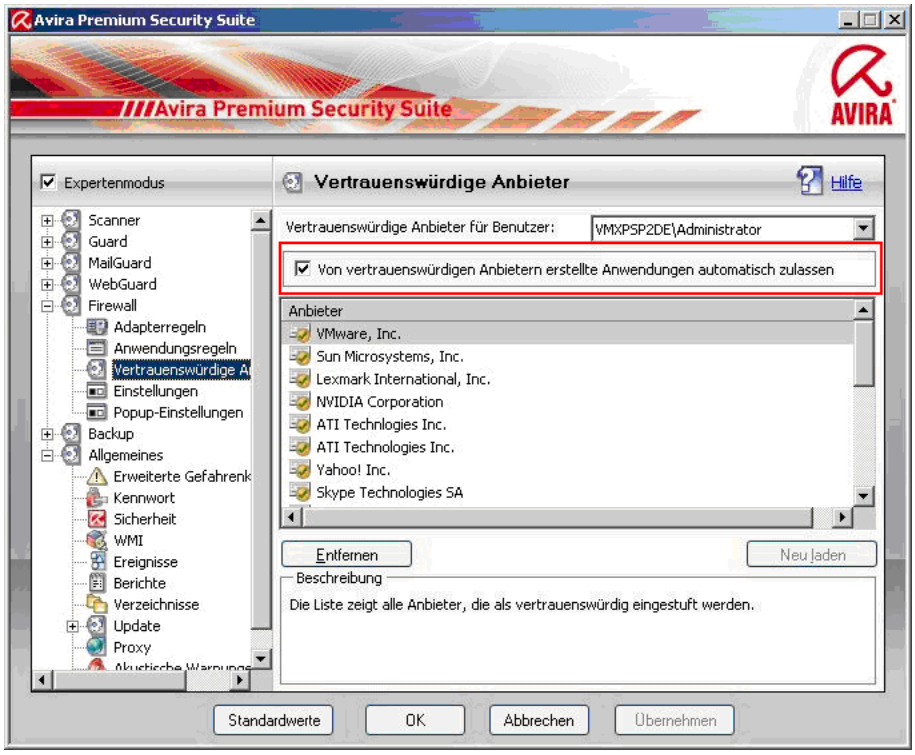
3.2.3.1 Vertrauenswürdige Anbieter für Benutzer

Diese Liste enthält alle Benutzer im System. Falls Sie als Administrator angemeldet sind, können Sie einen Benutzer auswählen, dessen Liste vertrauenswürdiger Anbieter Sie einsehen oder pflegen möchten. Falls Sie kein Benutzer mit privilegierten Rechten sind, zeigt Ihnen die Liste nur den aktuell angemeldeten Benutzer.



3.2.3.2 Von vertrauenswürdigen Anbietern erstellte Anwendungen automatisch zulassen

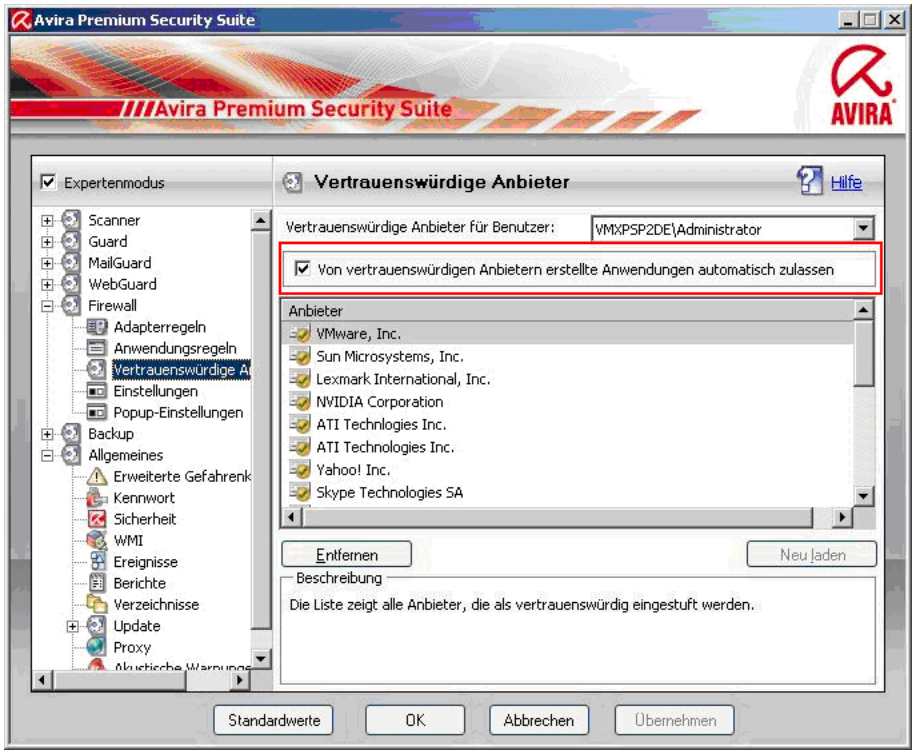
Bei aktivierter Option wird Anwendungen mit einer Signatur von bekannten und vertrauenswürdigen Anbietern automatisch der Zugang zum Netzwerk erlaubt. Die Option ist standardmäßig aktiviert.



Wir empfehlen Ihnen die Standardeinstellung aktiviert zu lassen. Da wir volle Kontaktdaten der Anbieter haben. Des weiteren handelt es sich hierbei um lizenzierte Softwarefirmen. Daher werden die Anbieter in der Liste von uns als vertrauenswürdig eingestuft.

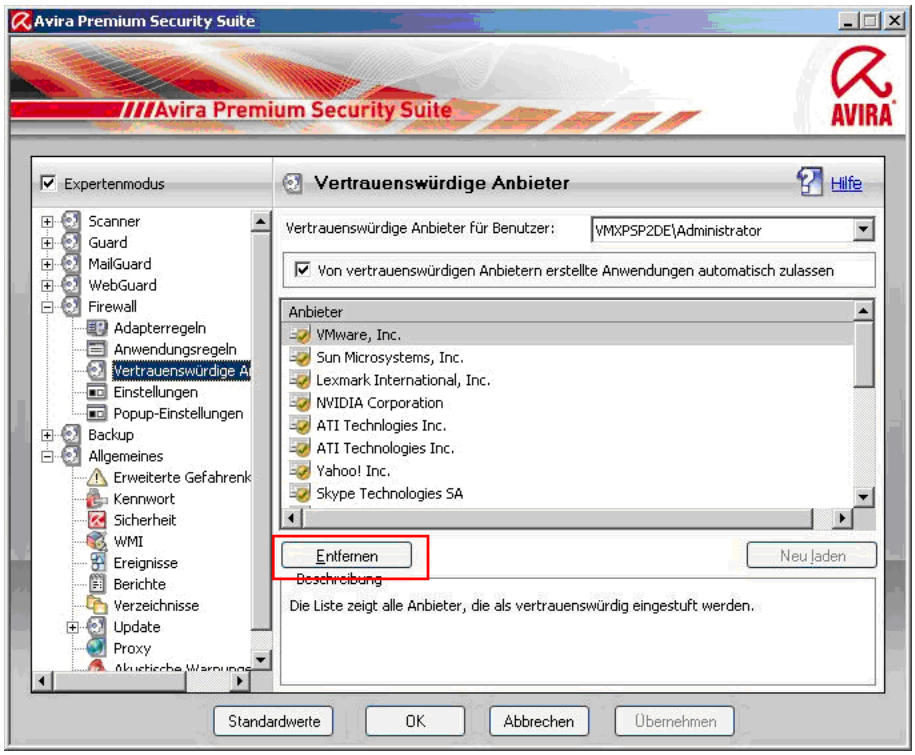
3.2.3.3 Anbieter

Die Liste zeigt alle Anbieter, die als vertrauenswürdig eingestuft werden.



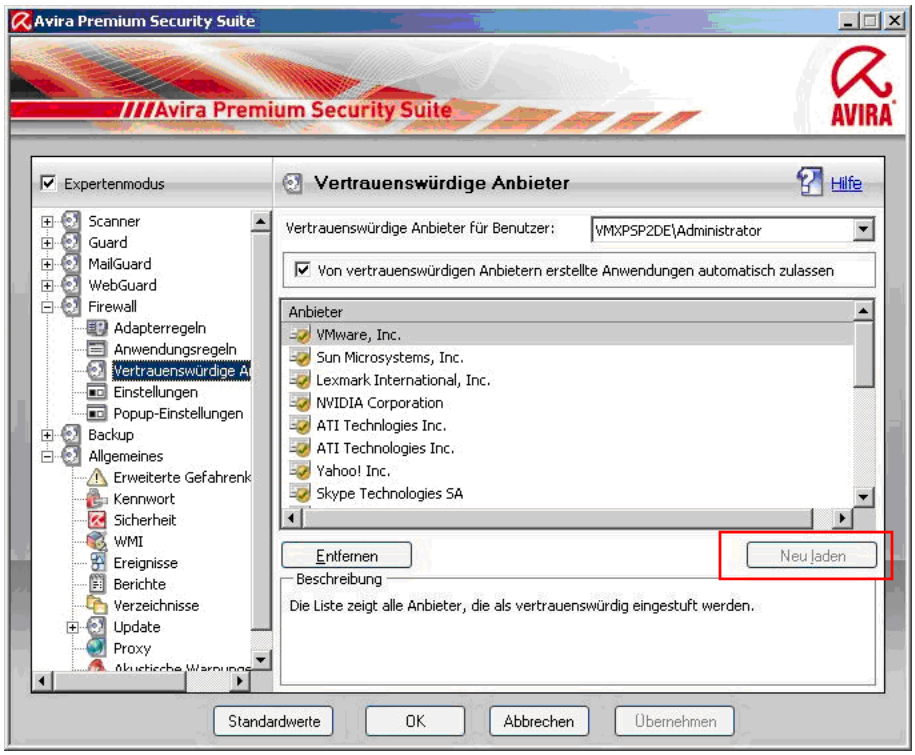
3.2.3.4 Entfernen

Der markierte Eintrag wird aus der Liste der vertrauenswürdigen Anbieter entfernt. Um den ausgewählten Anbieter endgültig aus der Liste zu entfernen, drücken Sie auf Übernehmen oder OK im Fenster der Konfiguration.



3.2.3.5 Neu laden

Die vorgenommenen Änderungen werden rückgängig gemacht: Die letzte gespeicherte Liste wird geladen.



Hinweis:

Wenn Sie Anbieter aus der Liste entfernen und anschließend die Schaltfläche Anwenden drücken, werden die Anbieter endgültig aus der Liste gelöscht. Die Änderung kann nicht mit Neuladen rückgängig gemacht werden. Sie haben jedoch die Möglichkeit, über die Option „Diesem Anbieter immer vertrauen“ im Popup-Fenster Netzwerkereignis einen Anbieter wieder zur Liste der vertrauenswürdigen Anbieter hinzuzufügen.

Die Firewall priorisiert Anwendungsregeln vor den Einträgen in der Liste der vertrauenswürdigen Anbieter: Wenn Sie eine Anwendungsregel erstellt haben und der Anbieter der Anwendung ist in der Liste der vertrauenswürdigen Anbieter aufgeführt, wird die Anwendungsregel ausgeführt.

3.2.4 Einstellungen

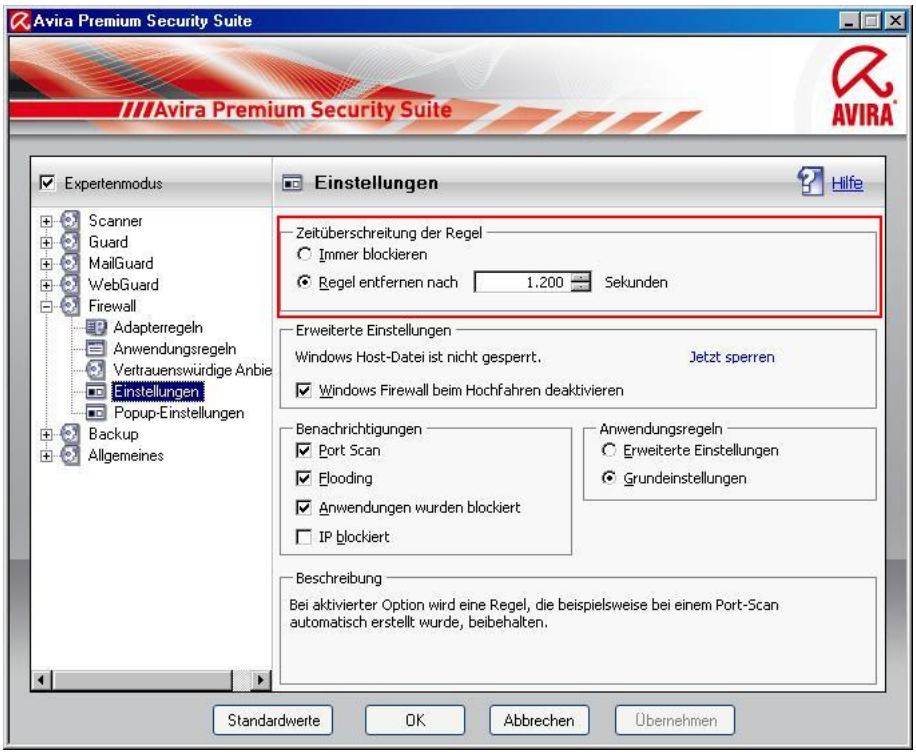
3.2.4.1 Zeitüberschreitung der Regel

- Immer blockieren

Bei aktivierter Option wird eine Regel, die beispielsweise bei einem Portscan automatisch erstellt wurde, beibehalten.

- Regel entfernen nach n Sekunden

Bei aktivierter Option wird eine Regel, die beispielsweise bei einem Portscan (siehe Begriffserklärung) automatisch erstellt wurde, nach der von Ihnen angegebenen Zeit wieder entfernt. Diese Option ist standardmäßig aktiviert.

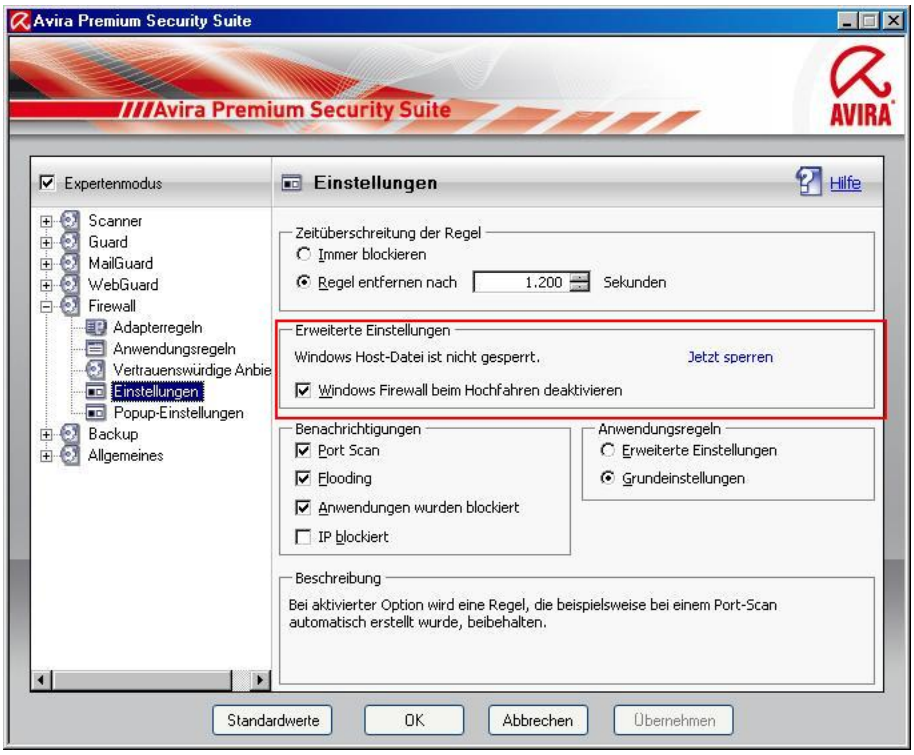


3.2.4.2 Erweiterte Einstellungen

- Windows Host-Datei ist NICHT GESPERRT/GESPERRT

Steht diese Option auf GESPERRT, ist die Windows Host-Datei schreibgeschützt. Eine Manipulation der Datei ist dann nicht länger möglich. Malware ist dann beispielsweise nicht mehr in der Lage, Sie auf unerwünschte Webseiten umzuleiten. Standardmäßig ist diese Option auf NICHT GESPERRT eingestellt.

Wir empfehlen Ihnen, die Windows Host-Datei auf GESPERRT zu stellen. Sollten Sie aber Anwendungen haben, die auf die Host-Datei zugreifen müssen, wie z.B. Spybot Search & Destroy, stellen Sie diese auf NICHT GESPERRT ein.

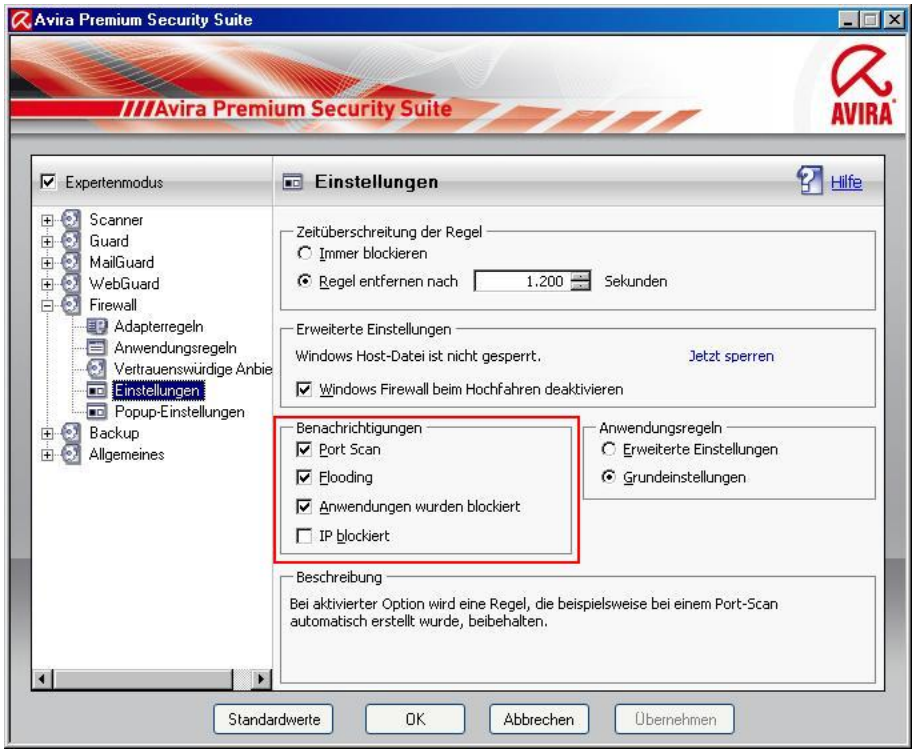


- Windows Firewall beim Hochfahren deaktivieren

Bei aktivierter Option ist die Windows Firewall beim Hochfahren des Rechners deaktiviert. Diese Option ist standardmäßig aktiviert, da die Verwendung von zwei gleichzeitig laufenden Desktop Firewalls unter Umständen Probleme hervorrufen kann. Zwei Desktop Firewalls behindern sich gegenseitig.

3.2.4.3 Benachrichtigungen

Unter Benachrichtigungen legen Sie fest, bei welchen Ereignissen Sie eine Desktopbenachrichtigung der Firewall erhalten möchten.



- Portscan

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn von der Firewall ein Portscan erkannt wurde.
Portscans sind in der Regel nicht unbedingt schädlich, deuten aber darauf hin, dass eventuell ein Angriff auf Ihr System stattfinden kann.

- Flooding

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn von der Firewall eine Flooding-Attacke erkannt wurde. Flooding-Attacken können unter Umständen Ihr Netzwerk mit Datenmengen „überfluten“, und Ihr Netzwerk lahmlegen.

- Anwendungen wurden blockiert

Sollte eine Anwendung versuchen, eine Verbindung nach außen herzustellen, die Sie nicht in der Firewall zugelassen haben, oder die nicht privilegiert ist, dann wird Sie von der Avira Firewall blockiert und Sie bekommen eine Desktopbenachrichtigung. In dieser Benachrichtigung wird Ihnen die Anwendung und der Grund der Blockade mitgeteilt.

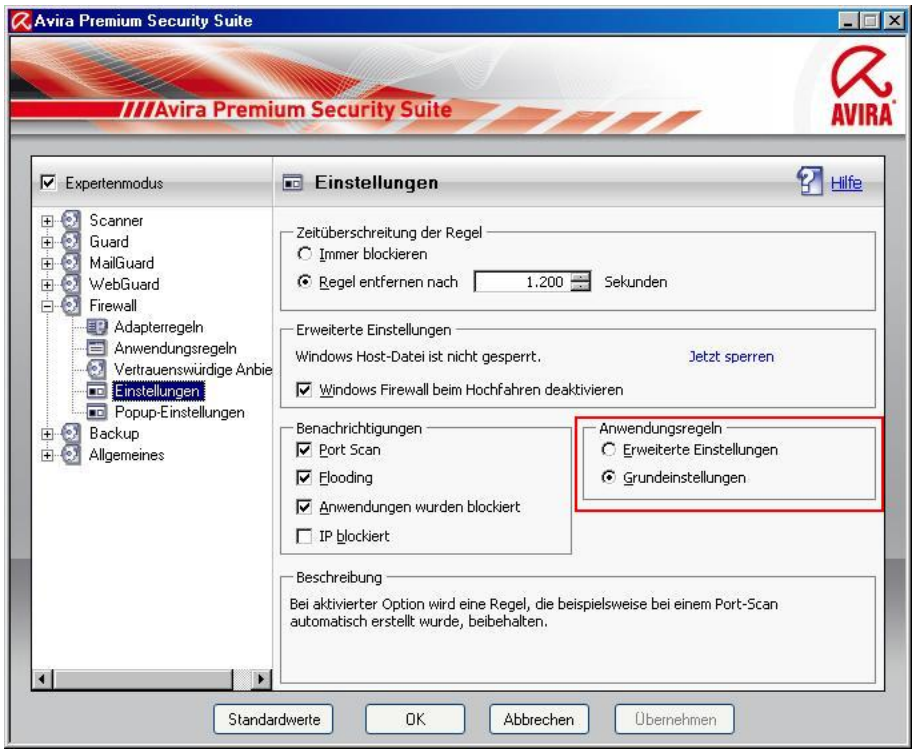
- IP blockiert

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn die Firewall den Datenverkehr von einer IP-Adresse zurückgewiesen hat. *Wir empfehlen diese*

Option nicht zu aktivieren, da es im Internet sehr häufig ungewollte IP Adressanfrage auf Rechner gibt, und Sie deshalb ständig Desktopmeldungen erhalten würden.

3.2.4.4 Anwendungsregeln

Mit den Optionen im Bereich Anwendungsregeln stellen Sie die Konfigurationsmöglichkeiten für Anwendungsregeln unter der Rubrik Firewall → Anwendungsregeln ein.



- Erweiterte Einstellungen

Bei aktivierter Option haben Sie die Möglichkeit, verschiedene Netzwerkzugänge einer Anwendung individuell zu regeln, d.h. hier haben Sie die Möglichkeit, einer Anwendung eine eigene Anwendungsregel zu erstellen. Sie können den Verkehr der Anwendung individuell regeln oder die Anwendung nur abhören.

- Grundeinstellungen

Bei aktivierter Option kann nur eine einzige Aktion für verschiedene Netzwerkzugänge der Anwendung eingestellt werden. Das reicht in der Regel aus, um Anwendungen zuzulassen oder zurückzuweisen.

3.2.5 Popup Einstellungen

3.2.5.1 Popup Einstellungen

- Startblock des Prozesses überprüfen

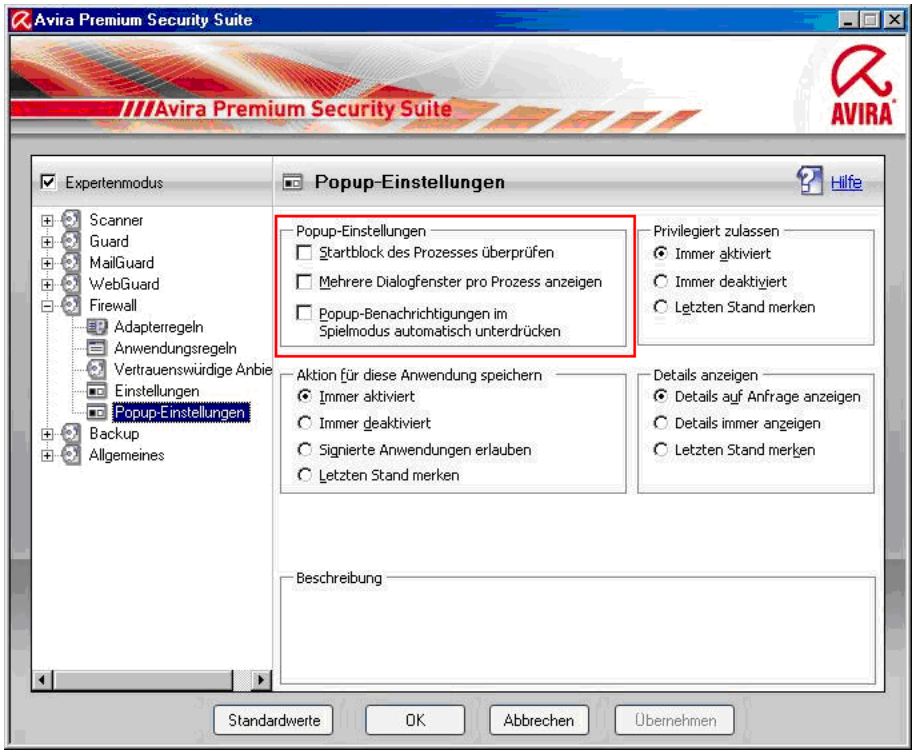
Bei aktivierter Option erfolgt eine präzisere Überprüfung des Prozessstapels. Die Firewall geht dann davon aus, dass jeder Prozess im Stapel, der nicht vertrauenswürdig ist, derjenige ist, über dessen Kindprozess auf das Netzwerk zugegriffen wird. Deshalb wird in diesem Fall für jeden nicht vertrauenswürdigen Prozess im Stapel ein eigenes Popup-Fenster geöffnet. Diese Option ist standardmäßig deaktiviert. *Wir empfehlen Ihnen, diese Standardeinstellung beizubehalten, da Sie sonst mit einer Flut von Popups rechnen müssen.*

- Mehrere Dialogfenster pro Prozess anzeigen

Bei aktivierter Option wird jedes Mal, wenn eine Anwendung versucht, eine Netzwerkverbindung herzustellen, ein Popup-Fenster geöffnet. Alternativ erfolgt die Information nur beim ersten Verbindungsversuch. Diese Option ist standardmäßig deaktiviert. *Wir empfehlen Ihnen diese Standardeinstellungen beizubehalten, damit Sie pro Prozess nur ein Popup-Fenster erhalten.*

- Popup-Benachrichtigung im Spielmodus automatisch unterdrücken

Bei aktivierter Option schaltet Avira Firewall automatisch in den Spielmodus um, wenn auf Ihrem Computersystem eine Anwendung im Vollbildmodus ausgeführt wird. Im Spielmodus werden alle definierten Adapter- und Anwendungsregeln angewendet. Anwendungen, für die keine Regeln mit den Aktionen Zulassen oder Zurückweisen definiert sind, wird der Netzwerkzugriff temporär erlaubt, so dass keine Popup-Fenster mit Abfragen zum Netzwerkereignis geöffnet werden. *Wir empfehlen Ihnen, falls Sie Spiele (Onlinespiele) auf Ihrem Rechner spielen, diese Option zu aktivieren, damit Sie während des Spiels nicht von lästigen Popups gestört werden.*



3.2.5.2 Aktion für diese Anwendung speichern

- Immer aktiv

Bei aktivierter Option ist die Option "Aktion für diese Anwendung speichern" des Dialogfensters "Netzwerkereignis" standardmäßig aktiviert. Diese Option ist standardmäßig aktiviert.

- Immer deaktiviert

Bei aktivierter Option ist die Option "Aktion für diese Anwendung speichern" des Dialogfensters "Netzwerkereignis" standardmäßig deaktiviert.

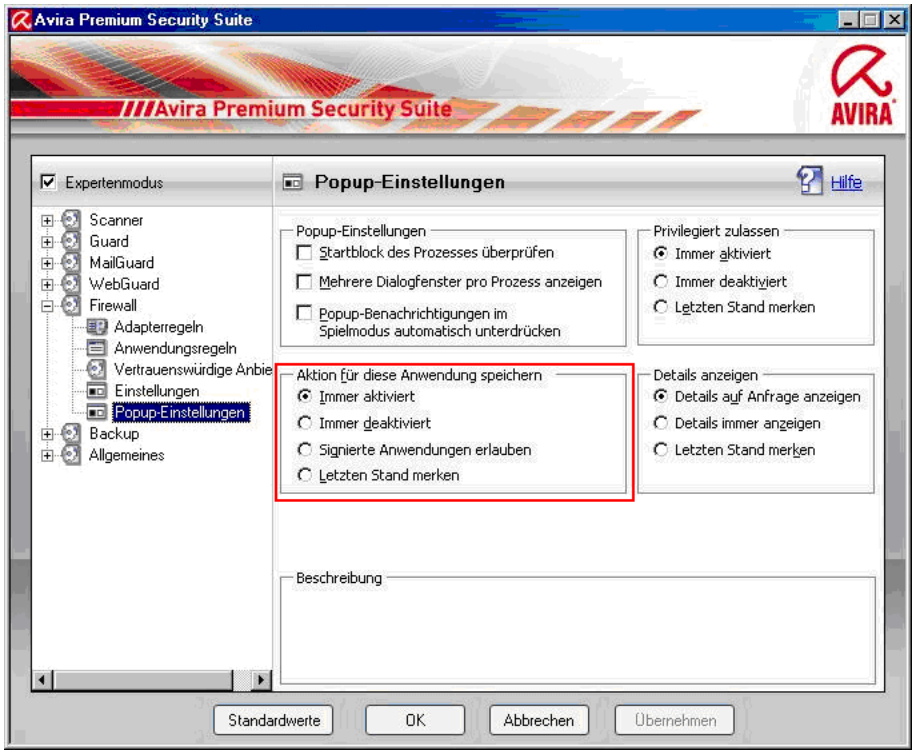
- Signierte Anwendung erlauben

Bei aktivierter Option ist beim Netzzugriff signierter Anwendungen bestimmter Hersteller die Option "Aktion für diese Anwendung speichern" des Dialogfensters "Netzwerkereignis" automatisch aktiviert. Die Hersteller sind: Microsoft, Mozilla, Opera, Yahoo, Google, Hewlet Packard, Sun, Skype, Adobe, Lexmark, Creative Labs, ATI, nVidia.

- Letzten Stand merken

Bei aktivierter Option wird die Aktivierung der Option "Aktion für diese Anwendung speichern" des Dialogfensters "Netzwerkereignis" gehandhabt wie beim letzten

Netzwerkereignis. Wurde beim letzten Netzwerkereignis die Option "Aktion für diese Anwendung speichern" aktiviert, ist die Option beim folgenden Netzwerkereignis aktiv. Wurde beim letzten Netzwerkereignis die Option "Aktion für diese Anwendung speichern" deaktiviert, ist die Option beim folgenden Netzwerkereignis deaktiviert.



Wir empfehlen Ihnen, diese Option beizubehalten, damit alle Ihre Aktionen in Verbindung mit der jeweiligen Anwendung automatisch gespeichert werden.

3.2.5.3 Details anzeigen

In dieser Gruppe von Konfigurationsoptionen können Sie die Anzeige von Detailinformationen im Fenster Netzwerkereignis einstellen.

- Details auf Anfrage anzeigen

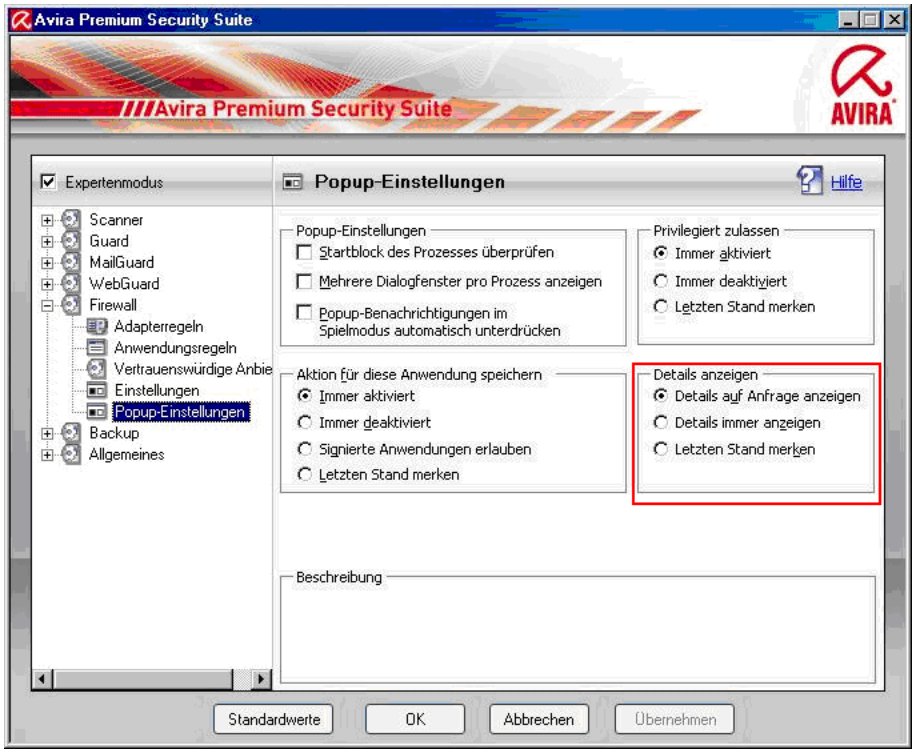
Bei aktivierter Option werden die Detailinformationen im Fenster Netzwerkereignis nur auf Anfrage angezeigt, d.h. eine Anzeige der Detailinformationen erfolgt mit Klick auf die Schaltfläche „Details einblenden“ im Fenster Netzwerkereignis.

- Details immer anzeigen

Bei aktivierter Option werden die Detailinformationen im Fenster Netzwerkereignis immer angezeigt.

- Letzten Stand merken

Bei aktivierter Option wird die Anzeige von Detailinformationen gehandhabt wie beim vorangegangenen Netzwerkereignis. Wurden beim letzten Netzwerkereignis Detailinformationen angezeigt oder abgerufen, werden beim folgenden Netzwerkereignis Detailinformationen angezeigt. Wurden beim letzten Netzwerkereignis die Detailinformationen nicht angezeigt oder ausgeblendet, werden beim folgenden Netzwerkereignis die Detailinformationen nicht angezeigt.



3.2.5.4 Privilegierte zulassen

In dieser Gruppe von Konfigurationsoptionen können Sie den Status der Option Privilegiert zulassen im Fenster Netzwerkereignis einstellen.

- Immer aktiviert

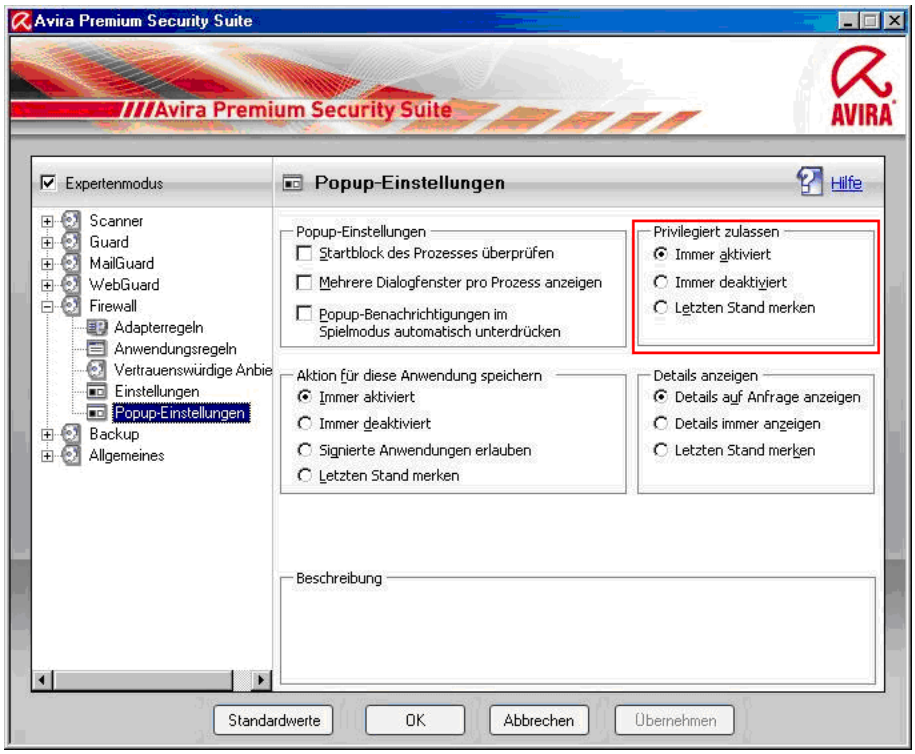
Bei aktivierter Option ist die Option Privilegierte zulassen im Fenster Netzwerkereignis standardmäßig aktiviert.

- Immer deaktiviert

Bei aktivierter Option ist die Option Privilegierte zulassen im Fenster Netzwerkereignis standardmäßig deaktiviert.

- Letzten Stand merken

Bei aktivierter Option wird der Status der Option „Privilegiert zulassen“ im Fenster Netzwerkereignis gehandhabt wie beim vorangegangenen Netzwerkereignis: War bei der Ausführung des letzten Netzwerkereignisses die Option Privilegiert zulassen aktiviert, ist beim folgenden Netzwerkereignis die Option standardmäßig aktiviert. War bei der Ausführung des letzten Netzwerkereignisses die Option Privilegiert zulassen deaktiviert, ist beim folgenden Netzwerkereignis die Option standardmäßig deaktiviert.

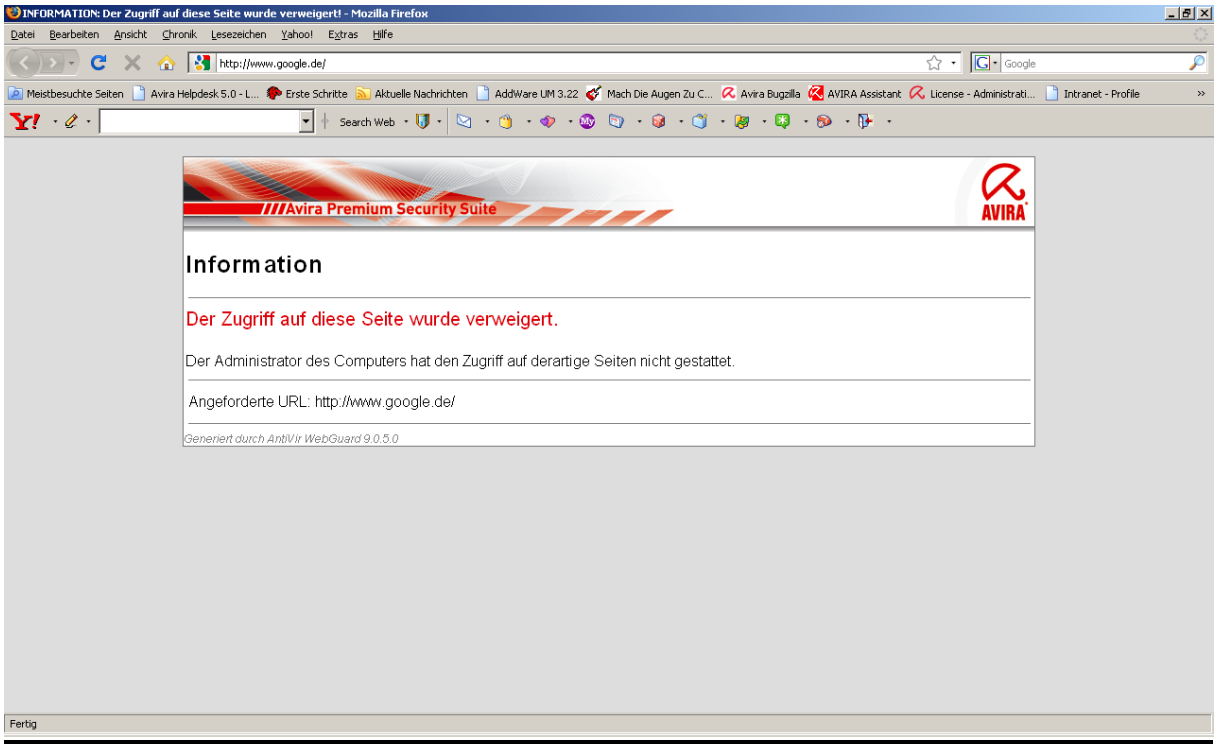


4. Allgemeines zum Kinderschutz

Premium Security Suite besitzt eine Kinderschutzfunktion zum Filtern unerwünschter oder illegaler Internetangebote. Den Benutzern des Computers können Nutzerrollen zugewiesen werden. Eine Nutzerrolle ist konfigurierbar und kann verbotene oder erlaubte URLs (Internetadressen) sowie verbotene Inhaltskategorien umfassen. Beim Blockieren von Internetinhalten nach bestimmten Kategorien werden leistungsstarke URL-Filterlisten verwendet, in denen URLs anhand der Inhalte der Internetseiten in Inhaltsgruppen kategorisiert sind. Die URL-Filterlisten werden täglich aktualisiert, angepasst und erweitert und unterstützen Sprachen aus dem europäischen Sprachraum (Deutsch, Englisch, Französisch, Italienisch, Russisch,...). Die Rollen Kind, Jugendlicher, Erwachsener sind mit den entsprechenden verbotenen Kategorien vorkonfiguriert. Um den Kinderschutz zu konfigurieren, müssen Sie den Kinderschutz aktivieren.
Ist der Kinderschutz aktiv, werden beim Navigieren im Internet alle im Browser angeforderten Webseiten anhand der Nutzerrolle geprüft. Bei verbotenen Webseiten wird die Webseite blockiert und eine Meldung im Browser angezeigt.

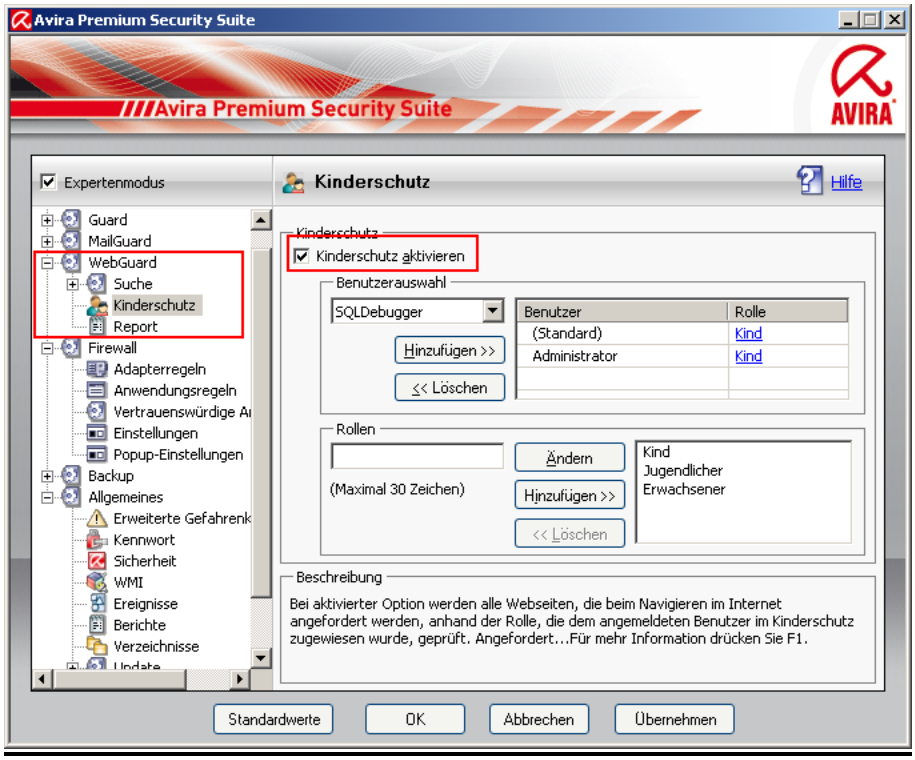
Beispiel:

Wenn eine gesperrte Seite aufgerufen wird, erscheint folgendes im Browserfenster.


INFORMATION: Der Zugriff auf diese Seite wurde verweigert! - Mozilla Firefox
Datei Bearbeiten Ansicht Chronik Lesezeichen Yahoo! Extras Hilfe
http://www.google.de/
Avira Premium Security Suite
AVIRA
Information
Der Zugriff auf diese Seite wurde verweigert.
Der Administrator des Computers hat den Zugriff auf derartige Seiten nicht gestattet.
Angeforderte URL: http://www.google.de/
Generiert durch AntiVir WebGuard 9.0.5.0
Fertig

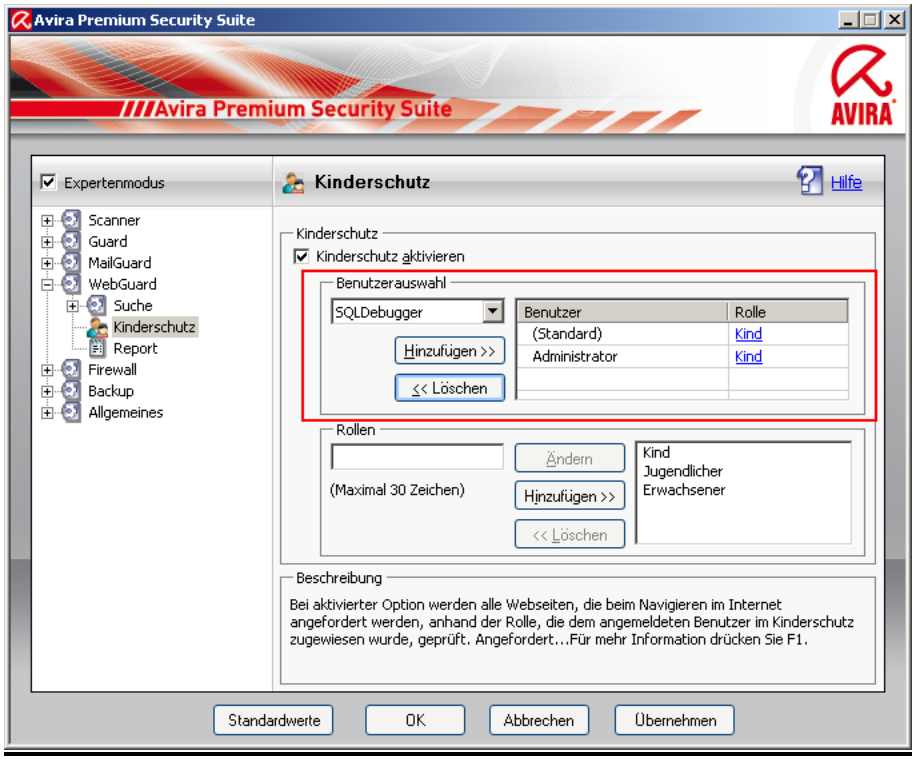
4.1 Kinderschutz aktivieren

Um den Kinderschutz zu aktivieren, gehen Sie in die Konfiguration von AntiVir und aktivieren Sie den Expertenmodus. Wählen Sie auf der linken Seite den Webguard aus. Sie öffnen den Baum, indem Sie auf das Plus vor Webguard klicken. Als dritten Punkt finden Sie den Kinderschutz. Wählen Sie diesen aus und aktivieren Sie ihn auf der linken Seite.



4.2 Benutzerauswahl

In dem Drop down Feld befinden sich alle Benutzer des Systems. Wählen Sie einen Benutzer aus und klicken auf „Hinzufügen“.
Der Benutzer erscheint links daneben mit der Standarteinstellung „Kind“. Sie können die Rolle des Benutzers durch einfaches Klicken ändern.



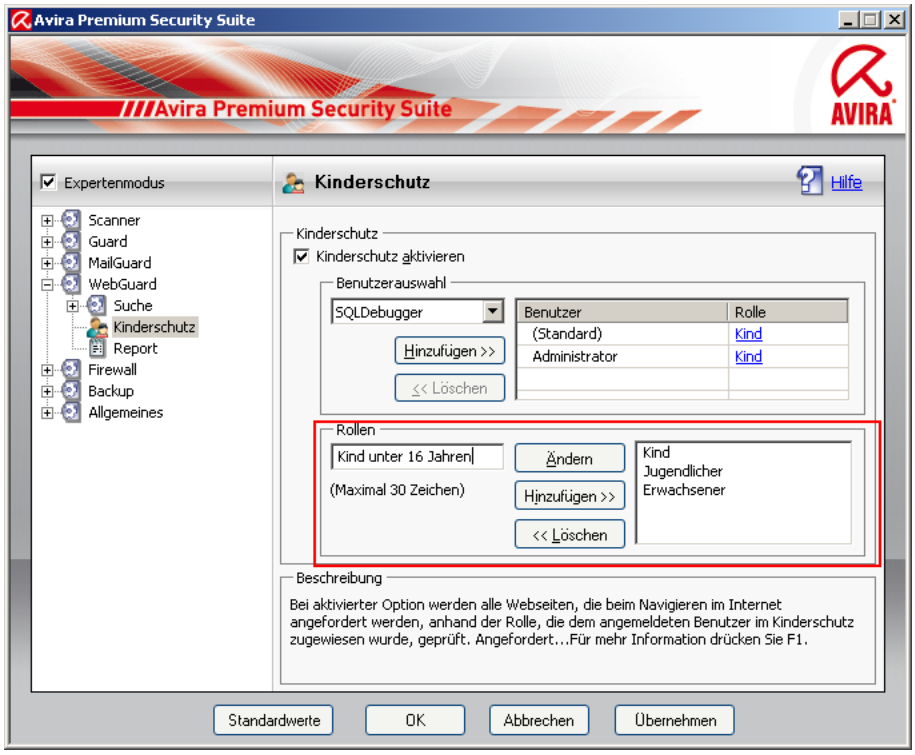
4.3 Rollen

Sie können entweder neue Rollen zu den bestehenden hinzufügen oder die bestehenden ändern.

Um neue Rollen hinzuzufügen, geben Sie den Rollennamen in das freie Feld ein. Beachten Sie, dass der Name nicht länger als 30 Zeichen sein darf.

Beispiel:

Kind unter 16 Jahren soll hinzugefügt werden.



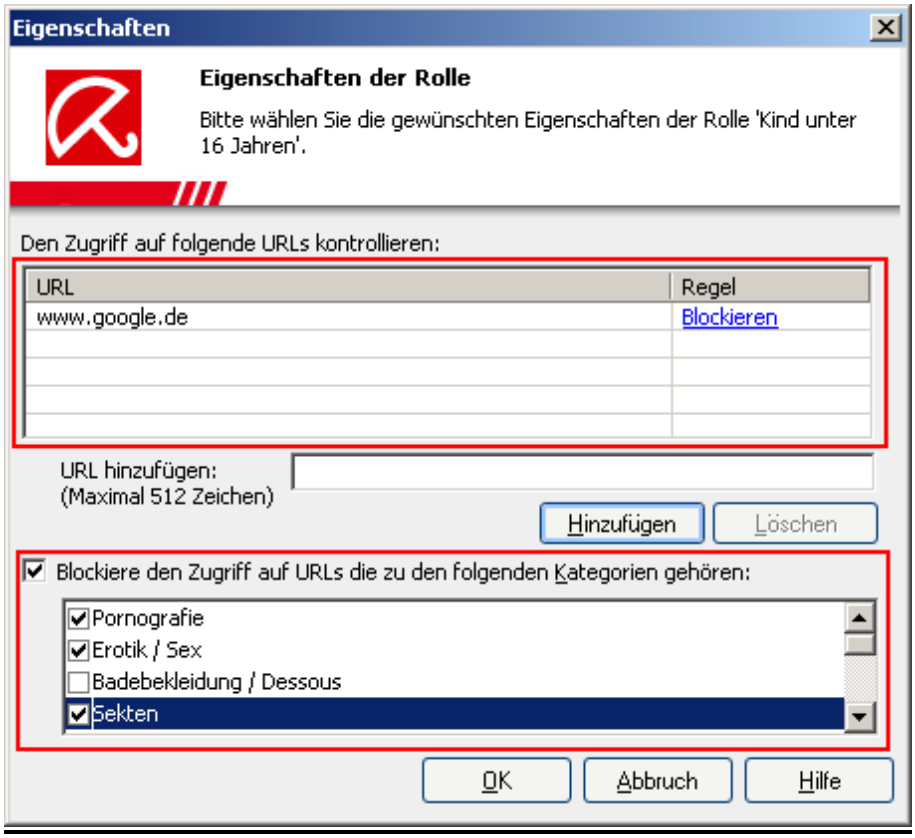
Klicken Sie auf „Hinzufügen“. Die neue Rolle erscheint im rechten Feld. Um die Rolle „Kind unter 16 Jahren“ zu konfigurieren, wählen Sie diese aus und klicken auf „Ändern“.

4.3.1 Eigenschaften von Rollen

Hier können Sie URLs hinzufügen und den Zugriff auf URLs, die zu bestimmten Kategorien gehören, sperren lassen.

Beispiel:

www.google.de und URLs der Kategorie *Pornografie, Erotik/Sex und Sekten* soll blockiert werden.



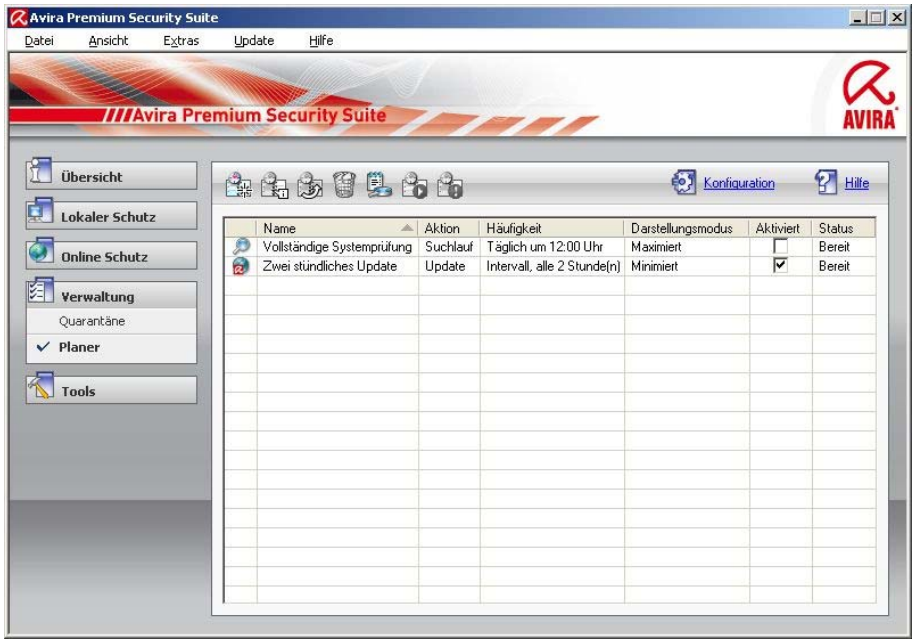
Die Kategorien wurden von einer riesigen Datenbank der Firma Cobion bereitgestellt. Des Weiteren greift der Webfilter auf eine Datenbank der Verbraucherschutzzentrale Hamburg zu. Sollte Ihnen eine Seite auffallen, die Ihres Erachtens auf eine Kategorie zutreffen sollte, können Sie diese über folgenden Link kategorisieren, bzw. überprüfen lassen: http://filterdb.iss.net/urlcheck/url-report.asp.

5. Änderung der Update-Intervalle

Das Update der Virendefinitionen ist im AntiVir Planer auf einen Intervall von zwei Stunden voreingestellt. Sollte ein anderer Zeitpunkt oder ein häufigeres Update erforderlich sein, kann diese Einstellung wie folgt verändert werden.

- Starten des Avira AntiVir Control Center (siehe S. 5)
- Aufruf des AntiVir Planers

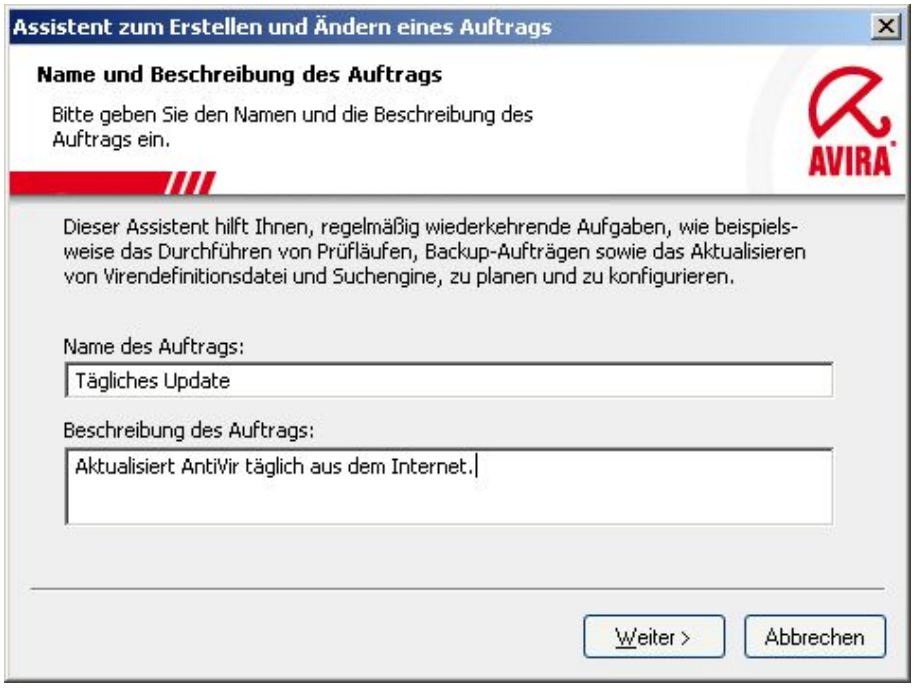
Klicken Sie in der AntiVir Benutzeroberfläche auf den Menüpunkt „Verwaltung“ auf der linken Seite. Klicken Sie hier auf den Eintrag „Planer“. Im Hauptfenster der Benutzeroberfläche erscheint jetzt die Planeroberfläche, in welcher alle eingestellten Update- oder Prüflaufaufträge angezeigt werden. Vorkonfiguriert sind hier das tägliche Update und die tägliche, vollständige Systemprüfung. Die vollständige Systemprüfung ist jedoch standardgemäß nicht aktiviert.



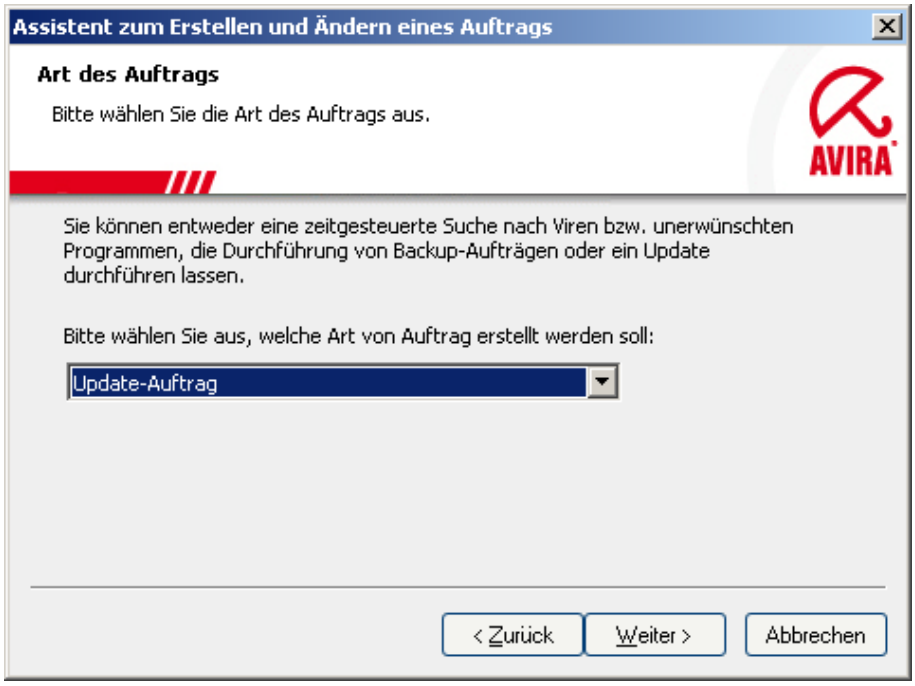
5.1 Änderung des Update-Auftrags

Klicken Sie mit der rechten Maustaste auf „Zwei stündliches Update“ und wählen Sie „Auftrag ändern“ aus dem Kontextmenü.

Es erscheint jetzt der Assistent zum Erstellen und Ändern eines Auftrags. Zu sehen ist der Name und die Beschreibung des Auftrags. Bei Bedarf können Sie hier die Beschreibung Ihren Vorstellungen entsprechend anpassen.


Assistent zum Erstellen und Ändern eines Auftrags
Name und Beschreibung des Auftrags
Bitte geben Sie den Namen und die Beschreibung des Auftrags ein.
AVIRA
Dieser Assistent hilft Ihnen, regelmäßig wiederkehrende Aufgaben, wie beispielsweise das Durchführen von Prüfläufen, Backup-Aufträgen sowie das Aktualisieren von Virendefinitionsdatei und Suchengine, zu planen und zu konfigurieren.
Name des Auftrags:
Tägliches Update
Beschreibung des Auftrags:
Aktualisiert AntiVir täglich aus dem Internet.
Weiter >
Abbrechen

Durch einen Klick auf den „Weiter“ Button erscheint das Fenster zur Auswahl der Art des Auftrags. Hier ist bereits korrekt „Update-Auftrag“ eingestellt. Klicken Sie hier einfach auf „Weiter“ um zur Einstellung des Zeitpunkts des Updates zu gelangen.

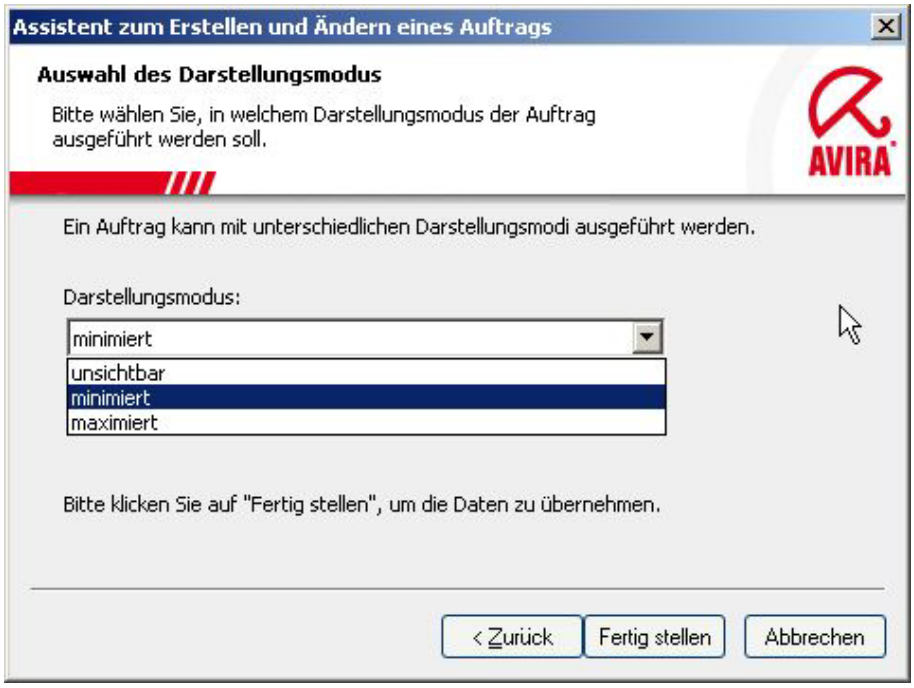

Assistent zum Erstellen und Ändern eines Auftrags
Art des Auftrags
Bitte wählen Sie die Art des Auftrags aus.
AVIRA
Sie können entweder eine zeitgesteuerte Suche nach Viren bzw. unerwünschten Programmen, die Durchführung von Backup-Aufträgen oder ein Update durchführen lassen.
Bitte wählen Sie aus, welche Art von Auftrag erstellt werden soll:
Update-Auftrag
< Zurück
Weiter >
Abbrechen

Assistent zum Erstellen und Ändern eines Auftrags
Zeitpunkt des Auftrags
Bitte wählen Sie aus, wann der Auftrag gestartet werden soll.
AVIRA
Ein Auftrag kann sofort, einmalig, beim Login sowie in unterschiedlichen Intervallen ausgeführt werden.
Bitte wählen Sie, wann dieser Auftrag ausgeführt werden soll:
Intervall
00 Tag(e) 02 Stunde(n) 00 Minute(n)
(min. 15 Minute(n))
Auftrag zusätzlich bei Internet Verbindung starten (DFÜ)
Auftrag nachholen, wenn die Zeit bereits abgelaufen ist
< Zurück
Weiter >
Abbrechen

Durch einen Klick auf das erste Einstellungsfeld ändern Sie die Einstellung von „Intervall“ nach „Täglich“. Im Feld darunter stellen Sie bitte den gewünschten Update-Zeitpunkt ein. Durch Aktivieren der Kästchen unterhalb können Sie noch festlegen, ob beim Aufbau einer DFÜ-Einwahlverbindung das Update gestartet werden soll. Falls das Update nachgeholt werden soll, da der Computer zum gewünschten Zeitpunkt nicht angeschaltet war, aktivieren Sie das zweite Kästchen.

Assistent zum Erstellen und Ändern eines Auftrags
Zeitpunkt des Auftrags
Bitte wählen Sie aus, wann der Auftrag gestartet werden soll.
AVIRA
Ein Auftrag kann sofort, einmalig, beim Login sowie in unterschiedlichen Intervallen ausgeführt werden.
Bitte wählen Sie, wann dieser Auftrag ausgeführt werden soll:
Täglich
12:00
Uhr
Auftrag zusätzlich bei Internet Verbindung starten (DFÜ)
Auftrag nachholen, wenn die Zeit bereits abgelaufen ist
< Zurück
Weiter >
Abbrechen

Klicken Sie auf „Weiter“, um zur Auswahl des Darstellungsmodus zu gelangen.



Klicken Sie auf das Auswahlfeld um die folgenden Darstellungsmodus auszuwählen:

- Unsichtbar: Das Update wird ohne jegliche Rückmeldung ausgeführt
- Minimiert: Das Update wird im Hintergrund durchgeführt und durch ein Slide-Up bestätigt
- Maximiert: Das Update wird mit vielen Details und großem Fenster dargestellt

Wählen Sie den gewünschten Modus aus und beenden Sie die Konfiguration mit einem Klick auf „Fertigstellen“.
Durch eine ähnliche Vorgehensweise lassen sich so auch Prüflauf-Aufträge einstellen und ändern. Hier muss lediglich anstelle „Update Auftrag“ die Einstellung „Prüfauftrag“ ausgewählt werden.

Ergänzungen zu diesem Dokument finden Sie:

- In der Onlinehilfe über das Programm (Taste F1)
- Im Benutzerhandbuch:

http://www.avira.com/documents/products/pdf/de/man_avira_premium_secrity_suite_de.pdf

- In unserer Wissensdatenbank:

http://www.avira.de/kb

- Unter FAQ (Häufig gestellte Fragen):

http://www.avira.de/faq